

A Difference Version of Nori's Theorem

Annette Maier

February 25, 2013

Abstract

We consider (Frobenius) difference equations over $(\mathbb{F}_q(s, t), \phi_q)$ where ϕ_q fixes t and acts on $\mathbb{F}_q(s)$ as the Frobenius endomorphism. We prove that every semisimple, simply-connected linear algebraic group \mathcal{G} defined over \mathbb{F}_q can be realized as a difference Galois group over $(\mathbb{F}_{q^i}(s, t), \phi_{q^i})$ for some $i \in \mathbb{N}$. The proof uses upper and lower bounds on the Galois group scheme of a Frobenius difference equation that are developed in this paper. The result can be seen as a difference analogue of Nori's Theorem which states that $\mathcal{G}(\mathbb{F}_q)$ occurs as (finite) Galois group over $\mathbb{F}_q(s)$.

1 Introduction

In analogy to the Galois theory of polynomials (or differential equations), *difference Galois theory* studies extensions generated by solutions of difference equations. A (linear) *difference equation* over a *difference field* (F, ϕ) (i.e., F is a field and ϕ an endomorphism of F) is an equation of the form

$$\phi(y) = Ay$$

with $A \in \mathrm{GL}_n(F)$, y a vector consisting of n indeterminates and ϕ applied coordinate-wise to y . A vector y with entries in a difference ring extension R of F (i.e., ϕ extends to R) satisfying $\phi(y) = Ay$ is called a *solution* of the difference equation. The term difference equation was originally only used over the difference field $\mathbb{C}(z)$ with $\phi : \mathbb{C}(z) \rightarrow \mathbb{C}(z)$ given by $\phi(z) = z + 1$. A classic example is the one-dimensional difference equation $\phi(y) = zy$ over $\mathbb{C}(z)$ which is solved by the Gamma function.

An equivalent concept to difference equations is that of *difference modules*. An n -dimensional difference module (M, Φ) over a difference field (F, ϕ) is an n -dimensional F -vector space together with a difference structure $\Phi : M \rightarrow M$ that is given by a matrix $D \in \mathrm{GL}_n(F)$ (with respect to a fixed basis \mathcal{B} of M): After identifying M with F^n via the basis \mathcal{B} , $\Phi(x) = D\phi(x)$ for $x \in M$; in other words, Φ acts *semilinearly* on M and D collects the images of \mathcal{B} in its columns. A *solution* of (M, Φ) is an element $x \in M \otimes_F R$ for some difference ring extension (R, ϕ) of (F, ϕ) such that $\Phi(x) = x$, where Φ acts on $M \otimes_F R$

via $\Phi \otimes \phi$. Note that the solutions of (M, Φ) are in bijection to the solutions of the difference equation $\phi(y) = D^{-1}y$. There is the notion of a *Picard-Vessiot ring* which is in some sense a “smallest” ring extension R of F together with an extension of ϕ such that there exists a full set of solutions in $M \otimes_F R$. In case the constants C of F (the elements fixed by ϕ) are algebraically closed, there always exists a Picard-Vessiot ring. The *difference Galois group* can then be defined as the group of automorphisms of R that leave F (pointwise) invariant and commute with ϕ ; it turns out to be a linear algebraic group defined over C (as developed in [vdPS97]). This can be generalized to the case of an arbitrary field of constants C , leading to difference Galois groups that are affine group schemes defined over C provided that there exists a Picard-Vessiot ring. The difference Galois group of an n -dimensional difference module can be embedded into GL_n .

Similar to the inverse problem in classical Galois theory, it is a natural question to ask which affine group schemes defined over C occur as Galois groups of some difference module over the fixed base field F with fixed endomorphism ϕ . For example, if $F = \mathbb{C}(z)$ with ϕ given by $\phi(z) = z + 1$ as above, it has been conjectured that a linear algebraic group \mathcal{G} over \mathbb{C} is a difference Galois group if and only if the quotient $\mathcal{G}/\mathcal{G}^0$ by the identity component is cyclic (it is known that this is true for $\mathcal{G} = \mathcal{G}^0$ and that the condition on $\mathcal{G}/\mathcal{G}^0$ is necessary - see [vdPS97]).

Let now $F = \mathbb{F}_q(s, t)$ be a function field in two variables over the finite field \mathbb{F}_q with $\phi = \phi_q$ acting trivially on $\mathbb{F}_q(t)$ and mapping s to s^q . Then the constants of F are $C = \mathbb{F}_q(t)$. Difference modules over (F, ϕ_q) are also called Frobenius modules. The **main result** of this paper is that every semisimple and simply-connected group \mathcal{G} that is defined over \mathbb{F}_q occurs as a ϕ_{q^i} -difference Galois group over $\mathbb{F}_{q^i}(s, t)$ for some $i \in \mathbb{N}$, (Theorem 6.6). The number i has to be chosen in such a way that the following holds:

- \mathcal{G} splits over \mathbb{F}_{q^i} and there exists a regular element $g_0 \in \mathcal{G}(\mathbb{F}_{q^i})$ contained in a maximal torus that splits over \mathbb{F}_{q^i}
- a certain place \mathfrak{p} of $\mathbb{F}_q(s)$ (depending on g_0) splits into places of degree 1 inside $\mathbb{F}_{q^i}(s)$.

It should be mentioned that in case $F = \overline{\mathbb{F}_q}(s)((t))$ with ϕ_q acting coefficient-wise as the Frobenius endomorphism on $\overline{\mathbb{F}_q}(s)$ (hence the constants of F equal $\mathbb{F}_q((t))$), the inverse problem has been solved by Matzat. Namely, Theorem 2.3 in [Mat09] implies that any linear algebraic group defined over $\mathbb{F}_q((t))$ occurs as a difference Galois group over $\overline{\mathbb{F}_q}(s)((t))$. However, this result is based on taking t -adic limits, so the proof cannot be transferred to our non-complete base field $\mathbb{F}_q(s)(t)$ or even $\overline{\mathbb{F}_q}(s)(t)$.

Our approach instead uses upper and lower bound techniques as follows. First, we give a necessary condition for the existence of a Picard-Vessiot ring of a Frobenius module (see Theorem 4.3 together with Theorem 2.5). Let (M, Φ) be

an n -dimensional Frobenius module with representing matrix $D \in \mathrm{GL}_n(\mathbb{F}_q(s, t))$ satisfying this condition and let $\mathcal{H} \leq \mathrm{GL}_n$ denote its Galois group. We show that given a connected linear algebraic group $\mathcal{G} \leq \mathrm{GL}_n$ defined over \mathbb{F}_q , we have $\mathcal{H} \leq \mathcal{G}$ if D is contained in $\mathcal{G}(\mathbb{F}_q(s, t))$ (Theorem 4.6 together with Proposition 2.13). This gives an upper bound on the difference Galois group \mathcal{H} . We also develop a lower bound criterion that yields explicit elements (depending on D) that are contained in \mathcal{H} up to conjugacy (see Theorem 4.12). These criteria can be used to construct Frobenius modules with given Galois group \mathcal{G} : Find a matrix $D \in \mathcal{G}(\mathbb{F}_q(s, t))$ (the representing matrix of the Frobenius module we are looking for) that meets the assumptions for the existence of a Picard-Vessiot ring such that any conjugates of the elements provided by our lower bound criterion generate \mathcal{G} (or a dense subgroup of \mathcal{G}); the latter condition requires a certain knowledge of how to generate \mathcal{G} . In this way, we derived explicit Frobenius modules with difference Galois groups SL_n , Sp_{2d} , SO_n and the Dickson groups G_2 in ([Mai11]).

Let now \mathcal{G} be an arbitrary semisimple and simply-connected group defined over \mathbb{F}_q . Nori's theorem ([Nor94]) asserts that $\mathcal{G}(\mathbb{F}_q)$ can be realized as finite Galois group over $\mathbb{F}_q(s)$. Using our three criteria explained above, we can “lift” this finite extension to a Frobenius module over $\mathbb{F}_q(s, t)$ with Galois group $\mathcal{H} \leq \mathcal{G}$ defined over $\mathbb{F}_q(t)$ such that every element in $\mathcal{G}(\mathbb{F}_q)$ occurs as constant coefficient matrix of some element inside $\mathcal{H}(\mathbb{F}_q[[t]])$, and such that \mathcal{H} contains a certain conjugate of a maximal torus T of \mathcal{G} that is defined over \mathbb{F}_q . By passing from \mathbb{F}_q to \mathbb{F}_{q^i} , we may assume that T splits over \mathbb{F}_q . Then we can use the structure theory of split reductive linear algebraic groups to show that any closed subgroup $\mathcal{H} \leq \mathcal{G}$ as above equals \mathcal{G} (Theorem 5.2).

We can also lift our difference modules from $\mathbb{F}_q(s, t)$ to $\overline{\mathbb{F}_q(s)}(t)$ to get difference modules with the same Galois group. As a result we obtain *rigid analytically trivial pre- t -motives* with arbitrary semisimple, simply-connected Galois groups. The category of rigid analytically trivial pre- t -motives contains the category of t -motives, which is of importance in the number theory of function fields (see for example [Pap08]).

The paper is organized as follows. Section 2 provides some background on the Galois theory of difference modules (with not necessarily algebraically closed fields of constants) collecting all statements used later. In Section 3, we set up some notation that will be used throughout all following sections. In Section 4, we develop techniques to guarantee that a Frobenius module has a certain difference Galois group. Specifically, Section 4.1 is concerned with the existence of Picard-Vessiot rings, while Sections 4.2 and 4.3 provide upper and lower bounds for difference Galois groups. Section 5 deals with finding generators of reductive groups that respect a certain conjugacy. Using the results from Sections 4 and 5, we can prove the main result in Section 6. In the last section, we translate the result to the language of pre- t -motives.

Acknowledgements

The author would like to thank J. Hartmann for many valuable suggestions and discussions, as well as D. Harbater, B.H. Matzat and M. Wibmer for helpful comments.

2 Basics of Difference Galois Theory

In this section we give a short introduction to the Galois theory of difference modules (in other words, the Galois theory of (linear) difference equations). The standard reference is [vdPS97]; unfortunately, the authors restrict themselves to algebraically closed fields of constants and surjective difference homomorphisms (“inversive” difference fields). Arbitrary fields of constants (but still in the inversive case) are treated in [AM05]. A more general approach is taken in [Wib10] which allows certain non-linear difference equations. Most of the statements quoted in this section can be proven similarly to the classical case (inversive and algebraically closed fields of constants). They also follow from the more general theory in [Wib10]. Direct proofs can be found in [Mai11].

Definition 2.1. A difference ring (R, ϕ) is a commutative ring R equipped with a ring homomorphism $\phi: R \rightarrow R$. A difference field is a difference ring which is a field. The constants C_R of a difference ring R are the elements of R fixed by ϕ . A difference ideal of a difference ring R is a ϕ -stable ideal of R and R is called a simple difference ring if its only difference ideals are (0) and R . In this case, C_R is a field. If R and S are difference rings, a ring homomorphism $\sigma: R \rightarrow S$ commuting with the difference structure on R and S is called a difference homomorphism. The set of all such is denoted by $\text{Hom}^\phi(R, S)$.

Example 2.2. Let q be a prime power and consider $\mathbb{F}_q(s, t)$. Let ϕ_q be the homomorphism on $\mathbb{F}_q(s, t)$ fixing t and restricting to the ordinary Frobenius endomorphism on $\mathbb{F}_q(s)$, i.e., $\phi_q(s) = s^q$. Then $\mathbb{F}_q(s, t)$ is a difference field extension of $\mathbb{F}_q(s)$, with constants $\mathbb{F}_q(t)$. Note that ϕ_q is not an automorphism.

Definition 2.3. Let (F, ϕ) be a difference field. A difference module (or ϕ -module, for short) over F is a finite dimensional F -vector space M together with a ϕ -semilinear map $\Phi: M \rightarrow M$, (i.e., Φ is additive and for any $\lambda \in F$ and $x \in M$ we have $\Phi(\lambda x) = \phi(\lambda)\Phi(x)$) such that there exists a representing matrix D contained in $\text{GL}_n(F)$, where $n = \dim_F(M)$. A representing matrix D is defined as follows: With respect to a fixed basis of M , the action of Φ is completely described by the images of the basis elements. The representing matrix D (with respect to this basis) collects these images in its columns. Conversely, every $D \in \text{GL}_n(F)$ gives rise to an n -dimensional difference module.

A fundamental (solution) matrix for M in some difference ring extension $R \geq F$ is defined to be an element $Y \in \text{GL}_n(R)$ such that $D\phi(Y) = Y$ holds, where ϕ is applied coordinate-wise. There exists a Φ -invariant basis of $M \otimes_F R$ if and only if there exists a fundamental solution matrix $Y \in \text{GL}_n(R)$. Indeed, the elements in M represented by the columns of a fundamental matrix are Φ -invariant.

We now present the notion of Picard-Vessiot rings of difference equations (which do not necessarily exist if the field of constants is not algebraically closed).

Definition 2.4. Let (F, ϕ) be a difference field with constants C and let (M, Φ) be a difference module over (F, ϕ) with representing matrix $D \in \mathrm{GL}_n(F)$. An extension of difference rings R/F is called a Picard-Vessiot ring for M if the following holds:

- R is a simple difference ring.
- The field of constants of R is C .
- There exists a fundamental matrix $Y \in \mathrm{GL}_n(R)$, i.e., $D\phi(Y) = Y$.
- R is generated as F -algebra by $\{Y_{ij}, \det(Y)^{-1} \mid 1 \leq i, j \leq n\}$.

We will use the notation $F[Y, Y^{-1}] := F[Y_{ij}, \det(Y)^{-1} \mid 1 \leq i, j \leq n]$.

The next theorem guarantees the existence of Picard-Vessiot rings provided there exists a fundamental matrix contained in a difference field extension with no new constants.

Theorem 2.5. Let (F, ϕ) be a difference field with field of constants C and let M be a difference module over F . Assume that L/F is a difference field extension such that

- a) The field of constants of L is C ,
- b) There exists a fundamental matrix $Y \in \mathrm{GL}_n(L)$, i.e., $D\phi(Y) = Y$,

Then $R := F[Y, Y^{-1}] \subseteq L$ is a Picard-Vessiot ring for M and R is the only Picard-Vessiot ring for M that is contained in L .

Definition 2.6. In the situation as in Theorem 2.5, i.e., if R is an integral domain, we call $\mathrm{Quot}(R)$ a Picard-Vessiot extension for M .

Remark 2.7. Other than in differential theory, the existence of a Picard-Vessiot ring does not imply the existence of a Picard-Vessiot extension, since a difference Picard-Vessiot ring is not necessarily a domain (we only know that it is reduced). It is therefore more natural to work with the total quotient rings of Picard-Vessiot rings instead of the field of fractions. However, the (explicitly constructed) Picard-Vessiot rings of the difference modules considered in this paper will be domains, so Theorem 2.5 will be sufficient for our purpose.

We now give a construction of the Galois group scheme \mathcal{G} of a Picard-Vessiot ring R , which turns out to be a linear algebraic group under certain separability assumptions. We will not assume our Picard-Vessiot ring to be integral.

Definition 2.8. Let (F, ϕ) be a difference field with field of constants C and let R be a Picard-Vessiot ring for some difference module over F . We write $\underline{\mathrm{Aut}}(R/F)$ for the functor from the category of C -algebras to the category of groups sending a C -algebra S to the group $\mathrm{Aut}^\phi(R \otimes_C S / F \otimes_C S)$ of difference automorphisms fixing $F \otimes_C S$. Note that we consider $R \otimes_C S$ as difference ring via $\phi \otimes \mathrm{id}$.

The key ingredient to show that $\underline{\text{Aut}}(R/F)$ is representable is the following proposition.

Proposition 2.9. *Let (F, ϕ) be a difference field with constants C and let R/F be a Picard-Vessiot ring for a difference module over F . Then we have an R -linear isomorphism of difference rings*

$$R \otimes_F R \cong R \otimes_C C_{R \otimes_F R},$$

where $R \otimes_F R$ and $R \otimes_C C_{R \otimes_F R}$ are considered as difference rings via $\phi \otimes_F \phi$ and $\phi \otimes_C \text{id}$, resp.

Theorem 2.10. *The group functor $\underline{\text{Aut}}(R/F)$ is represented by the C -algebra $C_{R \otimes_F R}$, and is thus an affine group scheme over C . If moreover R is separable over F , then $\mathcal{G} = \underline{\text{Aut}}(R/F)$ is a linear algebraic group over C , that is, an affine group scheme of finite type over C , such that $\mathcal{G} \times_C \overline{C}$ is reduced (i.e., \mathcal{G} is “geometrically reduced”).*

Definition 2.11. *Let (F, ϕ) be a difference field with field of constants C and let (M, Φ) be a difference module over (F, ϕ) with a Picard-Vessiot ring R . Then we call $\underline{\text{Aut}}(R/F)$ the Galois group scheme of M (with respect to R , which is not unique, in general). Two different Picard-Vessiot rings for the same difference module yield Galois groups that are isomorphic over an algebraic closure of C .*

As a corollary to Proposition 2.9, we get the well-known identity between transcendence degree of Picard-Vessiot extensions and dimension of their Galois group scheme:

Corollary 2.12. *Let (F, ϕ) be a difference field with field of constants C and let R be a Picard-Vessiot ring for a difference module over (F, ϕ) with Galois group scheme \mathcal{G} . Then $R \otimes_F \overline{F} \cong C[\mathcal{G}] \otimes_C \overline{F}$, where \overline{F} denotes an algebraic closure of F . In particular, $\dim(R) = \dim(\mathcal{G})$, where $\dim(R)$ denotes the Krull dimension of R .*

An explicit linearization of $\mathcal{G} = \underline{\text{Aut}}(R/F)$ can be given using a fundamental solution matrix:

Proposition 2.13. *Let R be a Picard-Vessiot ring for a difference module over a difference field (F, ϕ) . Let C be the field of constants and let \mathcal{G} be the Galois group scheme. Assume further that R is separable over F . Then there is a closed embedding $\rho: \mathcal{G} \hookrightarrow \text{GL}_n$ of linear algebraic groups such that for any C -algebra S , we have*

$$\rho_S: \mathcal{G}(S) = \text{Aut}^\phi(R \otimes_C S/F \otimes_C S) \rightarrow \text{GL}_n(S), \quad \sigma \mapsto Y^{-1} \sigma(Y).$$

Proposition 2.13 becomes particularly useful for obtaining upper bounds on the Galois group \mathcal{G} : Let R/F be a separable Picard-Vessiot ring with Galois group scheme \mathcal{G} . Assume that there exists a fundamental solution matrix Y that is contained in $\tilde{\mathcal{G}}(R)$ for some closed subgroup $\tilde{\mathcal{G}} \leq \text{GL}_n$ defined over C .

Then for all $\gamma \in \text{Aut}(R \otimes_C S/F \otimes_C S)$, $\gamma(Y)$ is contained in $\tilde{\mathcal{G}}(R \otimes_C S)$ and $\mathcal{G}_{R/F} \cong \rho(\mathcal{G}_{R/F})$ is thus contained in $\tilde{\mathcal{G}}$.

The following proposition consists of one direction of a Galois correspondence for difference modules and can be proven directly using Proposition 2.9.

Proposition 2.14. *Let (R, ϕ) be a Picard-Vessiot ring over a difference field (F, ϕ) with Galois group scheme \mathcal{G} . Let $\frac{a}{b}$ be an element in the total quotient ring of R (the localization at the set of all non zero divisors of R). If $\frac{a}{b}$ is functorially invariant under the action of \mathcal{G} , i.e., for every C -algebra S and every $\sigma \in \text{Aut}^\phi(R \otimes_C S/F \otimes_C S)$ we have*

$$\sigma(a \otimes_C 1) \cdot (b \otimes_C 1) = (a \otimes_C 1) \cdot \sigma(b \otimes_C 1),$$

then $\frac{a}{b}$ is contained in F .

As a consequence, we get the following lemma.

Lemma 2.15. *Let (M, Φ) be an m -dimensional difference module over a difference field (F, ϕ) , with Picard-Vessiot extension E , fundamental matrix $Y \in \text{GL}_m(E)$ and Galois group scheme $\mathcal{H} \leq \text{GL}_m$. Suppose that there exists a $0 \neq w \in C_F^m$ that spans an \mathcal{H} -stable line, i.e., for any C_F -algebra S , we have $\mathcal{H}(S) \cdot w \subseteq S \cdot w$. Then there exists an $\alpha \in E^\times$ such that $v := \alpha Y \cdot w \in F^m \cong M$ and $N := F \cdot v$ defines a Φ -stable submodule of M .*

We conclude this section with a theorem concerning base change of Picard-Vessiot rings. It can easily be proven using Corollary 2.12.

Theorem 2.16. *Let (F, ϕ) be a difference field and let R/F be a Picard-Vessiot ring for a difference module M over F such that its Galois group scheme \mathcal{G} is a connected linear algebraic group.*

If (\tilde{F}, ϕ) is an algebraic difference field extension of F such that \tilde{F} and R are both contained in some common difference field L without new constants, then $R \otimes_F \tilde{F}$ is a Picard-Vessiot ring over (\tilde{F}, ϕ) for $M \otimes_F \tilde{F}$ with Galois group scheme \mathcal{G} .

3 Notation

We define difference fields $k(t) \subseteq K(t) \subseteq L$ with field of constants $\mathbb{F}_q(t)$.

q	a power of a prime p .
k	a field containing \mathbb{F}_q with a fixed (non-trivial) non-archimedean absolute value $ \cdot $.
K	the completion of an algebraic closure of the completion of k with respect to $ \cdot $. Note that K is algebraically closed.
\bar{k}	the algebraic closure of k contained in K .
\bar{k}^{sep}	the separable algebraic closure of k contained in K .

$\mathcal{O}_{ \cdot }$	the valuation ring in K corresponding to $ \cdot $.
\mathfrak{m}	the maximal ideal inside $\mathcal{O}_{ \cdot }$.
$K\{t\}$	the ring of power series that converge on the closed unit disk: $K\{t\} := \{\sum_{i=0}^{\infty} \alpha_i t^i \in K[[t]] \mid \lim_{i \rightarrow \infty} \alpha_i = 0\}$.
L	the field of fractions of $K\{t\}$: $L = \text{Quot}(K\{t\})$.
(K, ϕ_q)	$\phi_q: K \rightarrow K$, $\lambda \mapsto \lambda^q$ is the ordinary Frobenius endomorphism on K . The field of constants then equals $C_K = \mathbb{F}_q$.
$(K((t)), \phi_q)$	The action of ϕ_q on Laurent series over K is defined coefficient-wise, i.e. $C_{K((t))} = \mathbb{F}_q((t))$.
(L, ϕ_q)	The action of ϕ_q on $K((t))$ induces a homomorphism on $L \subseteq K((t))$. The field of constants then equals $C_L = \mathbb{F}_q(t)$.
$(k(t), \phi_q)$	the difference structure on $k(t)$ is induced by that on $K(t) \subseteq L$, i.e., ϕ_q only acts on the coefficients of a rational function. Then $C_{k(t)} = \mathbb{F}_q(t)$ holds.
M_n	$n \times n$ -matrices.

Example 3.1. *The standard examples are $k = \mathbb{F}_q(s)$, a function field in one variable with an s -adic absolute value $|\cdot|$ or $k = \overline{\mathbb{F}_q(s)}$. One might also consider function fields $\mathbb{F}_q(s_1, \dots, s_n)$ in several variables with $|\cdot|$ for instance an s_1 -adic absolute value.*

Remark 3.2. *a) Note that $L/k(t)$ is usually not a separable extension (as K/k might not be separable), and thus $(\mathbb{F}_q(t), k(t), L)$ is not a ϕ_q -admissible triple as defined in [Pap08, 4.1.].*
b) Sometimes people work with the inverse σ of ϕ_q instead of ϕ_q , but since this is not defined on our base field $k(t)$ if k is not perfect, we prefer to work with ϕ_q , instead.

4 Bounds on Difference Galois Groups

In this section, we prove upper and lower bounds on the Galois group of a difference module over $(k(t), \phi_q)$ that only depend on a representing matrix of the difference module. These criteria are aimed to construct difference modules with prescribed Galois group schemes.

4.1 Existence of Picard-Vessiot Extensions

We first give a criterion (Theorem 4.3) that provides us with a fundamental solution matrix $Y \in \text{GL}_n(L)$ to a given difference module over $(k(t), \phi_q)$. Note that $Y \in \text{GL}_n(L)$ ensures the existence of a Picard Vessiot ring (see Theorem 2.5). We start with a multidimensional version of Hensel's Lemma. For $m \in \mathbb{N}$, let $\|\cdot\|$ denote the maximum norm on K^m induced by $|\cdot|$:

$$\|(a_1, \dots, a_m)\| := \max\{|a_i| \mid 1 \leq i \leq m\}.$$

Lemma 4.1 (Hensel's Lemma). *Let $f_1, \dots, f_m \in \mathcal{O}_{|\cdot|}[X_1, \dots, X_m]$ be a system of m polynomials in m variables with coefficients in $\mathcal{O}_{|\cdot|}$. Assume that there exists a vector $b = (b_1, \dots, b_m) \in \mathcal{O}_{|\cdot|}^m$ such that $\|(f_1(b), \dots, f_m(b))\| < |\det(J_b)|^2$, where $J_b = (\frac{\partial f_i}{\partial X_j}(b))_{i,j}$ denotes the Jacobian matrix at b . Then there is a unique $a \in \mathcal{O}_{|\cdot|}^m$ satisfying $f_i(a) = 0$ for all $1 \leq i \leq m$ and*

$$\|a - b\| = \frac{\|J_b^* \cdot (f_1(b), \dots, f_m(b))^{\text{tr}}\|}{|\det(J_b)|},$$

where J_b^* denotes the adjoint matrix of J_b .

This version of Hensel's Lemma is sometimes also called multi-dimensional Newton's Lemma. It holds for all henselian fields (note that K is henselian as it is complete with respect to a rank one valuation). For a proof, see Theorem 23 and 24 of [Kuh10].

Corollary 4.2. *Let A and B be contained in $M_n(\mathcal{O}_{|\cdot|})$ and consider the system of polynomial equations*

$$AY^q - Y + B = 0,$$

where $Y = (Y_{ij})_{i,j \leq n}$ consists of n^2 indeterminates and $Y^q := (Y_{ij}^q)_{i,j}$. Assume that there exists a $Y' \in M_n(\mathcal{O}_{|\cdot|})$ such that $\|A(Y')^q - Y' + B\| < 1$. Then there exists a unique solution $Y \in M_n(\mathcal{O}_{|\cdot|})$ of $AY^q - Y + B = 0$ such that $\|Y - Y'\| = \|A(Y')^q - Y' + B\|$.

Proof. This is an immediate consequence of Lemma 4.1. Indeed, let $f_{rs} \in \mathcal{O}_{|\cdot|}[Y_{ij} \mid 1 \leq i, j \leq n]$, $1 \leq r, s \leq n$ be the system of polynomials defining $AY^q - Y + B = 0$ and let A_{rs}, B_{rs} be the coordinates of A and B ($1 \leq r, s \leq n$). Then

$$f_{rs} = \sum_{m=1}^n A_{rm} Y_{ms}^q - Y_{rs} + B_{rs},$$

hence $\frac{\partial f_{rs}}{\partial Y_{ij}} = -\delta_{(i,j),(r,s)}$. This means that J_b equals the negative of the $n^2 \times n^2$ identity matrix for all $b \in M_n(K)$, so Y' meets the assumptions of the element b in Lemma 4.1. Also, up to a sign, $J_{Y'}^*$ equals the identity matrix, so the claim follows. \square

Theorem 4.3. *Let $D = \sum_{l=0}^{\infty} D_l t^l \in \text{GL}_n(\mathcal{O}_{|\cdot|}[[t]])$ (with $D_l \in M_n(\mathcal{O}_{|\cdot|})$) be such that there exists a $\delta < 1$ with*

$$\|D_l\| \leq \delta^l$$

for all $l \in \mathbb{N}$. Then there exists a fundamental matrix $Y \in \text{GL}_n(L)$ for D , i.e., $D\phi_q(Y) = Y$. More precisely, $Y = \sum_{l=0}^{\infty} Y_l t^l \in \text{GL}_n(\mathcal{O}_{|\cdot|}[[t]])$ with $Y_l \in M_n(\mathcal{O}_{|\cdot|})$ satisfying $\|Y_l\| \leq \delta^l$ for all $l \in \mathbb{N}$.

Proof. Observe that $D\phi_q(Y) = Y$ is equivalent to

$$D_0Y_l^q + D_1Y_{l-1}^q + \cdots + D_lY_0^q = Y_l \quad \text{for all } l \in \mathbb{N}.$$

We define $(Y_l)_{l \geq 0}$ inductively. For $l = 0$, we need to solve $D_0\phi_q(Y_0) = Y_0$. The Lang isogeny (see [Bor91, V.16.4]) asserts that such a Y_0 exists inside $\text{GL}_n(K)$, as K is algebraically closed. Then $Y_0^q = D_0^{-1}Y_0$ holds, hence $\mathcal{O}_{|\cdot|}[(Y_0)_{ij} \mid 1 \leq i, j \leq n]$ is finitely generated as an $\mathcal{O}_{|\cdot|}$ -module, since $D_0 \in \text{GL}_n(\mathcal{O}_{|\cdot|})$. Therefore, all entries of Y_0 are integral over $\mathcal{O}_{|\cdot|}$ and as $\mathcal{O}_{|\cdot|}$ is integrally closed inside K , we conclude that $\|Y_0\| \leq 1 = \delta^0$ holds. On the other hand, $D_0\phi_q(Y_0) = Y_0$ implies $\det(D_0)\det(Y_0)^q = \det(Y_0)$, hence $\det(Y_0)^{-1}$ is integral over $\mathcal{O}_{|\cdot|}$ which implies $\det(Y_0) \in \mathcal{O}_{|\cdot|}^\times$ and therefore $Y_0 \in \text{GL}_n(\mathcal{O}_{|\cdot|})$.

Now suppose that Y_0, \dots, Y_{l-1} have been chosen such that for all $1 \leq i \leq l-1$, $\|Y_i\| \leq \delta^i$ and $D_0Y_i^q + D_1Y_{i-1}^q + \cdots + D_iY_0^q = Y_i$ holds. We claim that we can find $Y_l \in \text{M}_n(\mathcal{O}_{|\cdot|})$ such that $D_0Y_l^q + D_1Y_{l-1}^q + \cdots + D_lY_0^q = Y_l$ and $\|Y_l\| \leq \delta^l$. Set $A := D_0 \in \text{GL}_n(\mathcal{O}_{|\cdot|})$ and $B := D_1Y_{l-1}^q + \cdots + D_lY_0^q \in \text{M}_n(\mathcal{O}_{|\cdot|})$. We have to find a solution to the polynomial system of equations

$$AY^q - Y + B = 0.$$

We have

$$\begin{aligned} \|B\| &= \|D_1Y_{l-1}^q + \cdots + D_lY_0^q\| \\ &\leq \max\{\|D_iY_{l-i}^q\| \mid 1 \leq i \leq l\} \\ &\leq \max\{\|D_i\| \cdot \|Y_{l-i}\|^q \mid 1 \leq i \leq l\} \\ &\leq \max\{\delta^i \cdot \delta^{(l-i)q} \mid 1 \leq i \leq l\} \\ &\leq \delta^l, \end{aligned}$$

where we used that the maximum norm $\|\cdot\|$ coming from a non-archimedean absolute value is sub-multiplicative with respect to the matrix multiplication. Let $\theta \in \mathcal{O}_{|\cdot|}$ be an element such that $|\theta| \leq \delta$ and set $Y'_l = \theta^l \cdot I_n$, where I_n denotes the identity matrix. Then we have

$$\|A(Y'_l)^q - Y'_l + B\| \leq \max\{\|A\| \cdot \|Y'_l\|^q, \|Y'_l\|, \|B\|\} \leq \delta^l < 1.$$

Hence by Corollary 4.2, there exists an element $Y_l \in \text{M}_n(\mathcal{O}_{|\cdot|})$ such that $AY_l^q - Y_l + B = 0$ and $\|Y_l - Y'_l\| = \|A(Y'_l)^q - Y'_l + B\| \leq \delta^l$. As $\|Y'_l\| \leq \delta^l$, we conclude $\|Y_l\| \leq \delta^l$.

The resulting matrix $Y = \sum_{l=0}^{\infty} Y_l t^l \in \text{M}_n(K\{t\}) \subseteq \text{M}_n(L)$ satisfies $D\phi_q(Y) = Y$ and $\|Y_l\| \leq \delta^l$ for all $l \in \mathbb{N}$. In particular, $Y \in \text{M}_n(\mathcal{O}_{|\cdot|}[[t]])$ and we have seen above that $Y_0 \in \text{GL}_n(\mathcal{O}_{|\cdot|})$, hence $Y \in \text{GL}_n(\mathcal{O}_{|\cdot|}[[t]])$. \square

4.2 An Upper Bound Theorem

Let F be a difference field with field of constants C_F and let \mathcal{G} be a connected linear algebraic group defined over C_F . For algebraically closed fields of constants it is well known that the Galois group of a difference module is contained

in \mathcal{G} if its representing matrix is contained in $\mathcal{G}(F)$ (see for example [vdPS03, Prop. 1.31]). In our setup of difference fields with a valuation and fields of constants $\mathbb{F}_q(t)$, we prove such a criterion under certain assumptions (see Theorem 4.6 below). The strategy is to show that there exists a fundamental matrix contained in \mathcal{G} if there exists one in GL_n . This implies that the Galois group scheme is contained in \mathcal{G} (see Prop. 2.13).

The Chevalley Theorem 4.4 has played an important role in solving the inverse problem in differential Galois theory (with algebraically closed constants). It has been used in characteristic zero (see [MS96]) as well as in the iterative differential case (see [Mat01]). We use it in the proof of both the upper and the lower bound theorem.

Theorem 4.4. *(Chevalley, see [Spr09, Theorem 5.5.3])*

Let \mathcal{G} be a linear algebraic group over an algebraically closed field F and \mathcal{H} a closed subgroup, both defined over a subfield $F_1 \subseteq F$. Then there exists an $m \in \mathbb{N}$ and a closed embedding $\rho: \mathcal{G} \rightarrow \mathrm{GL}_m$, which is defined over F_1 , such that there is a non-zero element $w \in F_1^m$ satisfying

$$\mathcal{H}(F) = \{g \in \mathcal{G}(F) \mid \rho(g)w \in Fw\}.$$

Note that the rational representation given in [Spr09] might not be a closed embedding itself, but it can be turned into one by taking the direct sum with an arbitrary closed embedding defined over F_1 .

Definition 4.5. *Assume that $\mathcal{O}_{|\cdot|}/\mathfrak{m}$ embeds into K . Then we can extend the canonical homomorphism $\kappa_{|\cdot|}: \mathcal{O}_{|\cdot|} \rightarrow \mathcal{O}_{|\cdot|}/\mathfrak{m}$ to a ring homomorphism*

$$\kappa_{|\cdot|}: \mathcal{O}_{|\cdot|}[[t]] \rightarrow (\mathcal{O}_{|\cdot|}/\mathfrak{m})[[t]] \rightarrow K[[t]],$$

by setting $\kappa_{|\cdot|}(\sum_{i=0}^{\infty} a_i t^i) = \sum_{i=0}^{\infty} \kappa_{|\cdot|}(a_i) t^i$ for any $a_i \in \mathcal{O}_{|\cdot|}$. Note that $\kappa_{|\cdot|}$ commutes with the action of ϕ_q on $K[[t]]$.

In Section 4.1 we constructed fundamental matrices $Y \in \mathrm{GL}_n(L) \cap \mathrm{M}_n(K\{t\})$. We will eventually need Y to be contained in $\mathcal{G}(K[[t]])$. Of course we still want to stay inside L (to ensure that we have no new constants) so we are looking for fundamental solution matrices contained in $\mathcal{G}(L \cap K[[t]])$. Note that $L \cap K[[t]] = \{\frac{f}{g} \mid f, g \in K\{t\}, t \nmid g\} \supsetneq K\{t\}$, for instance $(1-t)^{-1}$ is contained in $L \cap K[[t]]$ but $(1-t)$ is not invertible inside $K\{t\}$.

Theorem 4.6. *Assume that $\mathcal{O}_{|\cdot|}/\mathfrak{m}$ embeds into K . Let $\mathcal{G} \leq \mathrm{GL}_n$ be a connected linear algebraic group defined over \mathbb{F}_q . Let further $D = \sum_{l=0}^{\infty} D_l t^l \in \mathcal{G}(\mathcal{O}_{|\cdot|}[[t]])$ be such that $\|D_l\| < 1$ for all $l > 0$. Assume that there exists a matrix $Y \in \mathrm{GL}_n(\mathcal{O}_{|\cdot|}[[t]]) \cap \mathrm{M}_n(\mathcal{O}_{|\cdot|}\{t\})$ satisfying $D\phi_q(Y) = Y$. Then there exists a $Y' \in \mathcal{G}(L \cap \mathcal{O}_{|\cdot|}[[t]])$ with $D\phi_q(Y') = Y'$.*

Proof. For any matrix $A \in \mathrm{M}_n(\mathcal{O}_{|\cdot|}[[t]])$, we set $\tilde{A} := \kappa_{|\cdot|}(A)$ and similarly for vectors over $\mathcal{O}_{|\cdot|}[[t]]$ and scalars in $\mathcal{O}_{|\cdot|}[[t]]$.

By assumption, we have $\tilde{D} \in \mathcal{G}(K)$, i.e. no t appears. As K is algebraically closed, the Lang isogeny (see [Bor91, V.16.4]) asserts that there exists an $X \in \mathcal{G}(K)$ satisfying $\tilde{D}\phi_q(X) = X$. Now Y is contained in $\mathrm{GL}_n(\mathcal{O}_{|\cdot|}[[t]]) \cap \mathrm{M}_n(\mathcal{O}_{|\cdot|}\{t\})$, hence $\tilde{Y} \in \mathrm{GL}_n(K[[t]]) \cap \mathrm{M}_n(K[t]) \subseteq \mathrm{GL}_n(K(t))$. As $\kappa_{|\cdot|}$ and ϕ_q commute, we have $\tilde{D}\phi_q(\tilde{Y}) = \tilde{Y}$. Then $C := \tilde{Y}^{-1}X$ is contained in $\mathrm{GL}_n(C_{K(t)}) = \mathrm{GL}_n(\mathbb{F}_q(t))$.

We set $Y' := YC$. Clearly, $D\phi_q(Y') = Y'$ holds since C has constant entries. We claim that Y' is contained in $\mathcal{G}(L \cap \mathcal{O}_{|\cdot|}[[t]])$. First of all, Y has entries in $\mathcal{O}_{|\cdot|}\{t\} \subseteq L$ and C has entries in $\mathbb{F}_q(t) \subseteq L$, hence $YC \in \mathrm{GL}_n(L)$. Also, $\tilde{Y} \in \mathrm{GL}_n(K[[t]])$ and $X \in \mathrm{GL}_n(K)$, hence $C = \tilde{Y}^{-1}X \in \mathrm{GL}_n(K[[t]])$. We conclude $C \in \mathrm{GL}_n(\mathbb{F}_q(t)) \cap \mathrm{GL}_n(K[[t]]) \subseteq \mathrm{GL}_n(\mathbb{F}_q[[t]]) \subseteq \mathrm{GL}_n(\mathcal{O}_{|\cdot|}[[t]])$, thus $Y' = YC$ is also contained in $\mathrm{GL}_n(\mathcal{O}_{|\cdot|}[[t]])$. Therefore, it suffices to show that $Y' := YC$ is contained in $\mathcal{G}(\overline{K((t))})$.

By the Chevalley Theorem 4.4, there exists a closed embedding $\rho: \mathrm{GL}_n \rightarrow \mathrm{GL}_m$ defined over \mathbb{F}_q and a non-zero element $w \in \mathbb{F}_q^m$ such that

$$\mathcal{G}(\overline{K((t))}) = \{g \in \mathrm{GL}_n(\overline{K((t))}) \mid \rho(g)w \in \overline{K((t))} \cdot w\}. \quad (1)$$

By multiplying w by a suitable element in \mathbb{F}_q^\times , we may assume that there exists a $j \leq m$ such that $w_j = 1$.

Note that ρ commutes with both ϕ_q and $\kappa_{|\cdot|}$, as these both act trivially on \mathbb{F}_q . Also note that whenever a matrix A is contained in $\mathrm{GL}_n(\mathcal{O}_{|\cdot|}[[t]])$, $\rho(A)$ will be contained in $\mathrm{GL}_m(\mathcal{O}_{|\cdot|}[[t]])$, as ρ is defined over $\mathbb{F}_q \subseteq \mathcal{O}_{|\cdot|}$, hence both $\rho(A)$ and $\rho(A^{-1})$ have entries in $\mathcal{O}_{|\cdot|}[[t]]$.

We will show that there exist $v \in \mathbb{F}_q[[t]]^m$ and $\mu \in \mathcal{O}_{|\cdot|}[[t]]^\times$ such that

$$\rho(Y'^{-1})w = \mu v \quad (2)$$

holds. If this is true, we will have

$$\begin{aligned} \mu^{-1}\rho(Y'^{-1})w &= v = \kappa_{|\cdot|}(v) = \kappa_{|\cdot|}(\mu^{-1}\rho(Y'^{-1})w) = \tilde{\mu}^{-1}\rho(\tilde{Y}'^{-1})\tilde{w} \\ &= \tilde{\mu}^{-1}\rho(\tilde{C}^{-1}\tilde{Y}^{-1})w = \tilde{\mu}^{-1}\rho(C^{-1}\tilde{Y}^{-1})w = \tilde{\mu}^{-1}\rho(X^{-1})w, \end{aligned}$$

where we repeatedly used that $\kappa_{|\cdot|}$ acts trivially on $\mathbb{F}_q[[t]]$. Now $X^{-1} \in \mathcal{G}(K)$, hence $\rho(X^{-1})w \in Kw$ by (1). Also, $\tilde{\mu} \in K[[t]]^\times$ (as $\mu \in \mathcal{O}_{|\cdot|}[[t]]^\times$) so we conclude

$$\rho(Y'^{-1})w = \mu\tilde{\mu}^{-1}\rho(X^{-1})w \in K[[t]]w$$

which implies that $(Y')^{-1}$ and hence Y' is contained in $\mathcal{G}(\overline{K((t))})$ (see (1)).

It remains to show that there exist $v \in \mathbb{F}_q[[t]]^m$ and $\mu \in \mathcal{O}_{|\cdot|}[[t]]^\times$ satisfying Equation (2). First note that as $D \in \mathcal{G}(\mathcal{O}_{|\cdot|}[[t]]) \subseteq \mathcal{G}(\overline{K((t))})$, Equation (1) implies that there exists a $\lambda \in \overline{K((t))}$ satisfying

$$\rho(D)w = \lambda w.$$

We have $\rho(D) \in \mathrm{GL}_m(\mathcal{O}_{|\cdot|}[[t]])$, hence $\lambda = \lambda w_j = (\rho(D)w)_j \in \mathcal{O}_{|\cdot|}[[t]]$, as $w_j = 1$ and $w \in \mathbb{F}_q^m \subseteq \mathcal{O}_{|\cdot|}^m$. Similarly, $\lambda^{-1} = \lambda^{-1}w_j = (\rho(D)^{-1}w)_j \in \mathcal{O}_{|\cdot|}[[t]]$, hence λ is contained in $\mathcal{O}_{|\cdot|}[[t]]^\times$. We set $v' := \rho(Y'^{-1})w \in \mathcal{O}_{|\cdot|}[[t]]^m$ and compute

$$\begin{aligned}\phi_q(v') &= \phi_q(\rho(Y'^{-1})w) = \phi_q(\rho(Y'^{-1}))w = \rho(\phi_q(Y'^{-1}))w \\ &= \rho(Y'^{-1}D)w = \rho(Y'^{-1})\rho(D)w = \lambda v'.\end{aligned}\tag{3}$$

We can fix a $\mu \in \mathcal{O}_{|\cdot|}[[t]]^\times$ satisfying $\phi_q(\mu)\mu^{-1} = \lambda$. We define $v := \mu^{-1}v' = \mu^{-1}\rho(Y'^{-1})w$. Then $v \in \mathcal{O}_{|\cdot|}[[t]]^m$, and by Equation (3), we have

$$\phi_q(v) = \phi_q(\mu^{-1})\phi_q(v') = \phi_q(\mu^{-1})\lambda v' = v,$$

hence $v \in \mathbb{F}_q[[t]]^m$ and (v, μ) satisfy Equation (2) by definition. \square

4.3 Lower Bounds

We develop a lower bound criterion as follows. Let (M, Φ) be a difference module over $(\mathbb{F}_q(s, t), \phi_q)$ with representing matrix $D \in \mathrm{GL}_n(\mathbb{F}_q(s, t))$. Let \mathfrak{p} be a place of $\mathbb{F}_q(s)$ of degree $d \geq 1$ such that $D \in \mathrm{GL}_n(\mathfrak{o}[t]_{(t)})$, where \mathfrak{o} denotes the valuation ring corresponding to \mathfrak{p} . Then \mathcal{H} contains a certain conjugate of the reduction of $D\phi_q(D) \cdots \phi_q^{d-1}(D)$ modulo \mathfrak{p} (see Theorem 4.12). The criterion developed here actually works in the more general case $k(t) \supset \mathbb{F}_q(t)$ with k a (not necessarily discretely) valued field with finite residue field.

The idea to work with reductions at some places \mathfrak{p} to obtain elements of the Galois group up to conjugacy is inspired by finite Galois theory. Every finite Galois extension of $\mathbb{F}_q(s)$ is the Picard-Vessiot ring of a difference module over $(\mathbb{F}_q(s), \phi_q)$ (note that ϕ_q restricts to the ordinary Frobenius endomorphism on $\mathbb{F}_q(s)$). In [Mat04], Matzat gave a lower bound criterion for these kind of difference modules (so called finite Frobenius modules) using reductions of the representing matrix $D_0 \in \mathrm{GL}_n(\mathbb{F}_q(s))$ from $\mathbb{F}_q(s)$ to \mathbb{F}_q - this can be seen as a “linear Dedekind criterion”.

4.3.1 Setup for Specialization

In addition to the notation established in section 3, we will use the following notation in this section.

d	a fixed number $d \in \mathbb{N}$.
$(\mathfrak{o}, \mathfrak{p})$	a valuation ring \mathfrak{o} inside k with maximal ideal \mathfrak{p} such that the residue field $\mathfrak{o}/\mathfrak{p}$ is isomorphic to \mathbb{F}_{q^d} . We do not assume \mathfrak{o} to be discrete.
Γ	the corresponding ordered abelian group $\Gamma = k^\times / \mathfrak{o}^\times$.
$(\mathcal{O}, \mathcal{P})$	an extension of $(\mathfrak{o}, \mathfrak{p})$ to \bar{k}^{sep} .
Γ'	the corresponding ordered abelian group $\Gamma' := (\bar{k}^{\mathrm{sep}})^\times / \mathcal{O}^\times$.

ν	the corresponding valuation $\nu: \bar{k}^{\text{sep}} \rightarrow \Gamma' \cup \{\infty\}$. Note that ν restricts to $\nu: k \rightarrow \Gamma \cup \{\infty\}$.
κ	the residue homomorphism $\kappa: \mathcal{O} \rightarrow \bar{\mathbb{F}}_q$. (We have $\mathcal{O}/\mathfrak{p} \cong \bar{\mathbb{F}}_q$, as we assumed $\mathfrak{o}/\mathfrak{p} \cong \mathbb{F}_{q^d}$.) Note that κ restricts to $\kappa: \mathfrak{o} \rightarrow \mathbb{F}_{q^d}$.
ν_t	the Gauss extension $\nu_t: k(t) \rightarrow \Gamma \cup \{\infty\}$ of ν , defined by $\nu_t(\sum_{i=0}^r a_i t^i) = \min\{\nu(a_i) \mid 0 \leq i \leq r\}$ for $a_i \in k$ and $r \in \mathbb{N}$ and extended to fractions of polynomials.
$(\mathfrak{o}_t, \mathfrak{p}_t)$	the valuation ring \mathfrak{o}_t of ν_t inside $k(t)$ with maximal ideal \mathfrak{p}_t . The residue class field equals $\mathfrak{o}_t/\mathfrak{p}_t \cong \mathbb{F}_{q^d}(t)$ (see [EP05, Cor. 2.2.2]).
$\mathcal{O}((t))$	the ring of formal Laurent series over \mathcal{O} : $\mathcal{O}((t)) := \{\sum_{i=r}^{\infty} a_i t^i \mid r \in \mathbb{Z}, a_i \in \mathcal{O}\} = \mathcal{O}[[t]][t^{-1}]$.
\mathcal{O}_t	the subring of $\bar{k}^{\text{sep}}((t))$ generated by \mathfrak{o}_t and $\mathcal{O}((t))$. Since both $\mathcal{O}((t))$ and \mathfrak{o}_t are ϕ_q -stable inside $\bar{k}^{\text{sep}}((t))$, \mathcal{O}_t is ϕ_q -stable, as well. Also, note that $\mathbb{F}_q(t) \subseteq \mathcal{O}((t)) \subseteq \mathcal{O}_t$.
$(K((t)), \phi_q)$	we define ϕ_q on $K((t))$ (and any subring thereof) by setting $\phi_q(\sum_{i=r}^{\infty} a_i t^i) = \sum_{i=r}^{\infty} \phi_q(a_i) t^i = \sum_{i=r}^{\infty} a_i^q t^i$ for $r \in \mathbb{Z}$ and $a_i \in K$. This is compatible with the definition on the subfield L of $K((t))$ made in Section 3.

Remark 4.7. Note that \mathfrak{o}_t is not contained in $\mathcal{O}((t))$. Indeed, $\frac{1}{a+t}$ is contained in \mathfrak{o}_t but not in $\mathcal{O}((t))$, if $a \in \mathfrak{p} = \mathfrak{o} \setminus \mathfrak{o}^\times$.

Example 4.8. Note that $\mathfrak{o}/\mathfrak{p} \cong \mathbb{F}_{q^d}$ includes restrictions on k which had been an arbitrary subfield of K , before. For instance k cannot equal $\bar{\mathbb{F}}_q(s)$ anymore, since $\bar{\mathbb{F}}_q$ can be embedded into the residue field of any valuation on $\bar{\mathbb{F}}_q(s)$. In our application, $k = \mathbb{F}_q(s)$ with \mathfrak{p} a place of degree d . However, the results from this chapter could also be applied in more general situations such as $k = \mathbb{F}_q(s_1, \dots, s_r)$ with a rank- r -valuation ν and finite residue class field.

4.3.2 Specializing Fundamental Matrices

Lemma 4.9. Consider a system $AY^q - Y + B = 0$ of polynomial equations over \bar{k}^{sep} for an $A \in \text{GL}_n(\bar{k}^{\text{sep}})$ and $B \in \text{M}_n(\bar{k}^{\text{sep}})$, where Y denotes a matrix consisting of n^2 indeterminates. Let $Y \in K^{n \times n}$ be a solution. Then all entries of Y are contained in \bar{k}^{sep} .

Proof. This follows directly from the Jacobian criterion Proposition VIII.5.3. in [Lan02, Part II]. \square

Proposition 4.10. Let $D \in \text{GL}_n(\mathfrak{o}[[t]])$ and $Y \in \text{GL}_n(K[[t]])$ be such that $D\phi_q(Y) = Y$. Then Y is contained in $\text{GL}_n(\mathcal{O}[[t]])$.

Proof. We can write $D = \sum_{l=0}^{\infty} D_l t^l$ with $D_0 \in \text{GL}_n(\mathfrak{o})$ and $D_l \in \text{M}_n(\mathfrak{o})$ for all $l > 0$ and $Y = \sum_{l=0}^{\infty} Y_l t^l$ with $Y_0 \in \text{GL}_n(K)$ and all $Y_l \in \text{M}_n(K)$ for $l > 0$. Recall that $D\phi_q(Y) = Y$ is equivalent to

$$D_0 Y_l^q + D_1 Y_{l-1}^q + \dots + D_l Y_0^q = Y_l \text{ for all } l \in \mathbb{N}. \quad (4)$$

Inductively, we see that all entries of Y_l are contained in \bar{k}^{sep} , by Lemma 4.9. By induction, Y_l then satisfies an equation of the form $Y_l^q = D_0^{-1}Y_l + A$, where A has entries inside \mathcal{O} , hence $\mathcal{O}[(Y_l)_{i,j} \mid 1 \leq i, j \leq n]$ is finitely generated as an \mathcal{O} -module. Therefore, all entries of Y_l are integral over \mathcal{O} and thus contained in \mathcal{O} . It follows that Y is contained in $M_n(\mathcal{O}[[t]]) \cap \text{GL}_n(\bar{k}^{\text{sep}}[[t]])$ and $D_0 Y_0^q = Y_0$ implies $\det(Y_0) \in \mathcal{O}^\times$, hence $Y \in \text{GL}_n(\mathcal{O}[[t]])$. \square

Proposition 4.11. *We can extend the residue class homomorphism $\kappa: \mathcal{O} \rightarrow \bar{\mathbb{F}}_q$ to a homomorphism*

$$\kappa: \mathcal{O}_t \rightarrow \bar{\mathbb{F}}_q((t))$$

such that the following holds:

- a) κ commutes with ϕ_q .
- b) κ restricted to $\mathcal{O}((t))$ equals the coefficient-wise application of the residue map $\mathcal{O} \rightarrow \mathcal{O}/\mathcal{P} \cong \bar{\mathbb{F}}_q$ to a Laurent series over \mathcal{O} .
- c) κ restricts to the residue map $\mathfrak{o}_t \rightarrow \mathfrak{o}_t/\mathfrak{p}_t \cong \mathbb{F}_{q^d}(t)$ on \mathfrak{o}_t .

Proof. As the residue class homomorphism $\kappa: \mathcal{O} \rightarrow \bar{\mathbb{F}}_q$ is a homomorphism, it commutes with ϕ_q which is the ordinary Frobenius homomorphism on \mathcal{O} . We can extend κ to a ring homomorphism $\kappa: \mathcal{O}((t)) \rightarrow \bar{\mathbb{F}}_q((t))$ by applying κ to the coefficients of the Laurent series over \mathcal{O} . Since ϕ_q acts on \mathcal{O} coefficient-wise as well, we find that κ commutes with ϕ_q on $\mathcal{O}((t))$.

Let f be contained in \mathfrak{o}_t . Then f can be written as $\frac{g}{h}$ with $g \in \mathfrak{o}[t]$ and $h \in \mathfrak{o}[t] \cap \mathfrak{o}_t^\times$ and the residue map $\mathfrak{o}_t \rightarrow \mathbb{F}_{q^d}(t)$ maps f on $\frac{\kappa(g)}{\kappa(h)}$. We have

$$\begin{aligned} \mathcal{O}_t &= \left\{ \sum_{i=1}^n f_i g_i \mid n \in \mathbb{N}, f_i \in \mathcal{O}((t)), g_i \in \mathfrak{o}_t \right\} \\ &= \left\{ \sum_{i=1}^n \frac{f_i}{h_i} \mid n \in \mathbb{N}, f_i \in \mathcal{O}((t)), h_i \in \mathfrak{o}[t] \cap \mathfrak{o}_t^\times \right\} \\ &= \left\{ \frac{f}{h} \mid f \in \mathcal{O}((t)), h \in \mathfrak{o}[t] \cap \mathfrak{o}_t^\times \right\}. \end{aligned}$$

Setting $\kappa(\frac{f}{h}) = \frac{\kappa(f)}{\kappa(h)}$ yields a well-defined homomorphism on \mathcal{O}_t with all the desired properties. \square

4.3.3 A Lower Bound Theorem

Theorem 4.12. *Let $\mathcal{G} \leq \text{GL}_n$ be a linear algebraic group defined over $\mathbb{F}_q(t)$. Let (M, Φ) be an n -dimensional ϕ_q -module over $k(t)$ with representing matrix $D \in \mathcal{G}(k(t) \cap \mathfrak{o}[[t]])$. Assume that there exists a fundamental matrix $Y \in \mathcal{G}(K[[t]])$ for M generating a separable Picard-Vessiot extension $E/k(t)$ of M . Let $\mathcal{H} \leq \mathcal{G}$ be the Galois group-scheme of M corresponding to the Picard-Vessiot ring $R := k(t)[Y, Y^{-1}] \subseteq E$. Then $\mathcal{H}(\bar{\mathbb{F}}_q[[t]])$ contains a $\mathcal{G}(\bar{\mathbb{F}}_q[[t]])$ -conjugate of $\kappa(D\phi_q(D) \dots \phi_{q^{d-1}}(D))$.*

(More precisely, the conjugating matrix can be chosen as $\kappa(Y) \in \mathcal{G}(\bar{\mathbb{F}}_q[[t]])$).

Proof. We abbreviate $F := k(t)$ throughout this proof.

By Theorem 2.10, \mathcal{H} is a linear algebraic group and it is a subgroup of \mathcal{G} by Proposition 2.13. We apply Theorem 4.4 to \mathcal{G} and get a closed embedding $\rho: \mathcal{G} \rightarrow \mathrm{GL}_m$ defined over $\mathbb{F}_q(t)$ and a non-zero $w \in \mathbb{F}_q(t)^m$ such that

$$\mathcal{H}(S) = \{g \in \mathcal{G}(S) \mid \rho(g)w \in S \cdot w\} \quad (5)$$

holds for all $\mathbb{F}_q(t)$ -algebras S . We now blow up M to an m -dimensional version \tilde{M} in order to be able to apply Lemma 2.15. Let \tilde{M} be an m -dimensional difference module over F such that its representing matrix with respect to a fixed basis is given by $\rho(D) \in \mathrm{GL}_m(F)$. Then $\tilde{Y} := \rho(Y)$ is a fundamental solution matrix for \tilde{M} , since ρ is defined over $\mathbb{F}_q(t)$ and thus $\phi_q(\rho(Y)) = \rho(\phi_q(Y))$. All entries of \tilde{Y} are contained in R and furthermore, the entries of Y are contained in $F[\tilde{Y}, \tilde{Y}^{-1}]$, since ρ is a closed embedding defined over $\mathbb{F}_q(t) \subseteq F$. Hence $R = F[\tilde{Y}, \tilde{Y}^{-1}]$ is also a Picard-Vessiot ring for \tilde{M} and the Galois group scheme is $\rho(\mathcal{H}) \leq \mathrm{GL}_m$ in its natural representation as given in Proposition 2.13. By construction, w spans a $\rho(\mathcal{H})$ -stable line (see Equation (5)) and thus there exists an $\alpha \in E^\times$ such that

$$v = \alpha \tilde{Y} w \quad (6)$$

is contained in F^m and $N = Fv$ defines a difference submodule of \tilde{M} , by Lemma 2.15. This means that there exists a $\lambda \in F$ such that $\rho(D)\phi_q(v) = \lambda v$.

As $k(t) \cap \mathfrak{o}[[t]] \subseteq \mathfrak{o}_t$, D is contained in $\mathrm{GL}_n(\mathfrak{o}_t)$. Since ρ is defined over $\mathbb{F}_q(t) \subseteq \mathfrak{o}_t$, $\rho(D)$ and $\rho(D^{-1})$ both have coefficients in \mathfrak{o}_t and thus $\rho(D)$ is contained in $\mathrm{GL}_m(\mathfrak{o}_t)$.

Now fix an $i \leq m$ such that the i -th coordinate v_i of v has minimal valuation among all coordinates of v (with respect to ν_t and the order on Γ). After dividing v by v_i , we may assume $v_i = 1$. Thus $\lambda = \lambda \cdot v_i = (\rho(D)\phi_q(v))_i$ is contained in \mathfrak{o}_t since \mathfrak{o}_t is ϕ_q -stable. Also, $(\lambda)^{-1} = (\lambda)^{-1}\phi_q(v)_i = (\rho(D^{-1})v)_i$ is contained in \mathfrak{o}_t , so λ is in fact contained in \mathfrak{o}_t^\times . Overall, we got $\rho(D) \in \mathrm{GL}_m(\mathfrak{o}_t)$, $v \in \mathfrak{o}_t^m$ and $\lambda \in \mathfrak{o}_t^\times$, hence we may specialize them to $\kappa(\rho(D)) \in \mathrm{GL}_m(\mathbb{F}_{q^d}(t))$, $\kappa(v) \in \mathbb{F}_{q^d}(t)^m$ and $\kappa(\lambda) \in \mathbb{F}_{q^d}(t)^\times$, by Proposition 4.11.

We denote from now on the (coordinate-wise) application of κ to a matrix A with entries in \mathcal{O}_t by \overline{A} and similarly for vectors with entries in \mathcal{O}_t and scalars in \mathcal{O}_t . Applying κ to both sides of $\rho(D)\phi_q(v) = \lambda v$ coordinate-wise yields:

$$\overline{\rho(D)}\phi_q(\overline{v}) = \overline{\lambda} \cdot \overline{v}, \quad (7)$$

where we used that κ and ϕ_q commute (see Proposition 4.11) to get $\overline{\phi_q(v)} = \phi_q(\overline{v})$. Note that ρ commutes with the coordinate-wise application of κ to an element in $\mathcal{G}(\mathcal{O}_t)$, since ρ is defined over $\mathbb{F}_q(t)$ and κ restricts to the identity on $\mathbb{F}_q(t)$. In particular, $\overline{\rho(D)} = \rho(\overline{D})$ holds and we obtain $\rho(\overline{D}) \cdot \phi_q(\overline{v}) = \overline{\lambda} \cdot \overline{v}$. Inductively, we obtain

$$\rho(\overline{D})\phi_q(\rho(\overline{D})) \cdots \phi_{d-1}(\rho(\overline{D})) \cdot \overline{v} = \overline{\lambda}\phi_q(\overline{\lambda}) \cdots \phi_{q^{d-1}}(\overline{\lambda}) \cdot \overline{v}, \quad (8)$$

where we used $\phi_{q^d}(\bar{v}) = \bar{v}$. Proposition 4.10 implies that Y has entries in $\mathcal{O}[[t]]$, hence $\rho(Y)$ is contained in $\mathrm{GL}_m(\mathcal{O}((t))) \subseteq \mathrm{GL}_m(\mathcal{O}_t)$, as ρ is defined over $\mathbb{F}_q(t) \subseteq \mathcal{O}((t))$. There exists a $j \leq m$ such that $w_j \in \mathbb{F}_q(t)^\times \subseteq \mathcal{O}_t^\times$. Then Equation (6) implies $1 = v_i = \alpha \cdot (\rho(Y) \cdot w)_i$ and $(\rho(Y)^{-1} \cdot v)_j = \alpha \cdot w_j$ and we deduce that α is contained in \mathcal{O}_t^\times . It can thus be specialized to an element $\bar{\alpha} = \kappa(\alpha) \in \mathbb{F}_q((t))^\times$. We may apply κ to both sides of Equation (6) to get

$$\bar{v} = \bar{\alpha} \cdot \overline{\rho(Y)} \cdot \bar{w} = \bar{\alpha} \cdot \rho(\bar{Y}) \cdot w. \quad (9)$$

(Note that at this point we applied κ simultaneously to elements in $\mathcal{O}((t))$ and \mathfrak{o}_t which is why we had to construct κ on the somewhat peculiar ring \mathcal{O}_t in Proposition 4.11.)

Abbreviate $\hat{D} = D\phi_q(D) \cdots \phi_{q^{d-1}}(D)$ and $\hat{\lambda} = \lambda\phi_q(\lambda) \cdots \phi_{q^{d-1}}(\lambda)$. Then Equation (8) translates to

$$\rho(\bar{\hat{D}})\bar{v} = \bar{\hat{\lambda}}\bar{v}. \quad (10)$$

We now consider $\bar{Y}^{-1} \cdot \bar{\hat{D}} \cdot \bar{Y} = \kappa(Y^{-1}\hat{D}Y)$ which is contained in $\mathcal{G}(\mathbb{F}_q[[t]])$, since \mathcal{G} is defined over $\mathbb{F}_q(t)$ and κ acts trivially on $\mathbb{F}_q(t)$. We use Equation (9) and (10) to compute

$$\begin{aligned} \rho(\bar{Y}^{-1} \cdot \bar{\hat{D}} \cdot \bar{Y}) \cdot w &= \rho(\bar{Y}^{-1})\rho(\bar{\hat{D}})\rho(\bar{Y})w \\ &= \bar{\alpha}^{-1}\rho(\bar{Y}^{-1})\rho(\bar{\hat{D}})\bar{v} \\ &= \bar{\alpha}^{-1}\bar{\hat{\lambda}}\rho(\bar{Y}^{-1})\bar{v} \\ &= \bar{\hat{\lambda}} \cdot w. \end{aligned}$$

It follows that $\bar{Y}^{-1} \cdot \bar{\hat{D}} \cdot \bar{Y}$ is contained in $\mathcal{H}(\mathbb{F}_q[[t]])$ (see (5)). It remains to show that $\bar{Y}^{-1} \cdot \bar{\hat{D}} \cdot \bar{Y}$ has entries in $\mathbb{F}_q[[t]]$. To see this, recall that $D\phi_q(Y) = Y$ holds, hence $\bar{D}\phi_q(\bar{Y}) = \bar{Y}$ and $\phi_q(\bar{Y})^{-1} = \bar{Y}^{-1} \cdot \bar{D}$. We compute

$$\begin{aligned} \phi_q(\bar{Y}^{-1}\bar{\hat{D}}\bar{Y}) &= \phi_q(\bar{Y}^{-1})\phi_q(\bar{\hat{D}}) \cdots \phi_{q^d}(\bar{\hat{D}})\phi_q(\bar{Y}) \\ &= \phi_q(\bar{Y}^{-1})\phi_q(\bar{D}) \cdots \phi_{q^{d-1}}(\bar{D})\bar{D}\phi_q(\bar{Y}) \\ &= \bar{Y}^{-1}\bar{D}\phi_q(\bar{D}) \cdots \phi_{q^{d-1}}(\bar{D})\bar{Y} \\ &= \bar{Y}^{-1} \cdot \bar{\hat{D}} \cdot \bar{Y}, \end{aligned}$$

where we used $\bar{D} \in \mathrm{GL}_n(\mathbb{F}_{q^d}(t))$. Hence $\bar{Y}^{-1} \cdot \bar{\hat{D}} \cdot \bar{Y}$ has entries in $\mathbb{F}_q[[t]]^{\phi_q} = \mathbb{F}_q[[t]]$. \square

Example 4.13. If $k = \mathbb{F}_q(s)$ and $\mathfrak{p} = (s - \alpha)$ is a finite place of degree 1 ($\alpha \in \mathbb{F}_q$), then the Galois group scheme \mathcal{H} contains a conjugate of the specialized matrix $D_\alpha \in \mathcal{G}(\mathbb{F}_q(t))$ obtained by replacing each s occurring in $D \in \mathcal{G}(\mathbb{F}_q(s, t))$ by α .

5 Generating Split Reductive Groups

The lower bound criterion (Theorem 4.12) provides us with elements that are contained in the Galois group scheme up to conjugacy. In this section, we give generators of connected, reductive and \mathbb{F}_q -split groups that allow a certain conjugacy.

Proposition 5.1. *Let K_1 be an infinite field and let $\mathcal{G} \leq \mathrm{GL}_n$ be a connected linear algebraic group defined over K_1 such that either K_1 is perfect or \mathcal{G} is reductive. Let further K_2/K_1 be a field extension and consider the field of formal Laurent series $K_2((t))$ over K_2 . If $\mathcal{H} \subset \mathcal{G}$ is a closed subvariety defined over $K_2((t))$ such that for all $g \in \mathcal{G}(K_1)$ there exists an $h \in \mathcal{H}(K_2[[t]])$ of the form $h = g + M_1t + M_2t^2 + \dots$ for some $M_i \in M_n(K_2)$, then $\mathcal{H} = \mathcal{G}$ holds.*

Proof. First of all, note that $\mathcal{G}(K_1)$ is dense in \mathcal{G} , as we assumed that either K_1 is perfect or \mathcal{G} is reductive (see [Bor91, 18.3]).

Set $m = n^2 + 1$. Then \mathcal{G} is a closed subvariety of affine m -space, since $\mathcal{G} \leq \mathrm{GL}_n$ holds. Let $K_t := \overline{K_2((t))}$ be an algebraic closure of $K_2((t))$. We consider the vanishing ideals $I(\mathcal{G})$ and $I(\mathcal{H})$ of \mathcal{G} and \mathcal{H} inside $K_t[X_1, \dots, X_m]$. Assume that \mathcal{H} is strictly contained in \mathcal{G} , i.e., $I(\mathcal{H}) \supsetneq I(\mathcal{G})$. Now $I(\mathcal{H})$ is generated by finitely many elements inside $K_2((t))[X_1, \dots, X_m]$ and we conclude that at least one of them cannot be contained in $I(\mathcal{G})$. Let $f \in K_2((t))[X_1, \dots, X_m]$ be such an element, i.e., $f \in I(\mathcal{H}) \setminus I(\mathcal{G})$. After multiplying by a suitable power of t , we may assume that f is contained in $K_2[[t]][X_1, \dots, X_m] \subset K_2[X_1, \dots, X_m][[t]]$. Hence there exist elements $f_j \in K_2[X_1, \dots, X_m]$ such that

$$f = \sum_{j=0}^{\infty} f_j t^j.$$

As $\mathcal{G}(K_1)$ is dense in \mathcal{G} , there exists a $g \in \mathcal{G}(K_1)$ with $f(g) \neq 0$. It follows that there exists a $j \in \mathbb{N}$ such that $f_j(g) \neq 0$. Let $j_0 \in \mathbb{N}$ be minimal such that there exists a $g \in \mathcal{G}(K_1)$ with $f_{j_0}(g) \neq 0$. Hence f_0, \dots, f_{j_0-1} vanish on all $\mathcal{G}(K_1)$ and are thus contained in $I(\mathcal{G})$. Now consider

$$f' := t^{-j_0} \left(f - \sum_{j=0}^{j_0-1} f_j t^j \right) = f_{j_0} + f_{j_0+1}t + f_{j_0+2}t^2 + \dots$$

As $f \in I(\mathcal{H}) \setminus I(\mathcal{G})$ and $\sum_{j=0}^{j_0-1} f_j t^j \in I(\mathcal{G})$, we have $f' \in I(\mathcal{H}) \setminus I(\mathcal{G})$, as well. By definition of j_0 , there exists a $g \in \mathcal{G}(K_1)$ such that $f_{j_0}(g) \neq 0$. By assumptions, there exists an $h = g + M_1t + M_2t^2 + \dots \in \mathcal{H}(K_2[[t]])$ for some $M_i \in M_n(K_2)$, i.e., g occurs as the constant term of an element contained in $\mathcal{H}(K_2[[t]])$. We compute

$$0 = f'(h) = \sum_{j=0}^{\infty} f_{j+j_0}(h) t^j \in K_2[[t]]$$

and compare the constant terms of both sides. The constant term of the right hand side equals the constant term of $f_{j_0}(h)$ which in turn equals $f_{j_0}(g)$, hence $0 = f_{j_0}(g)$, a contradiction. Hence \mathcal{H} cannot be strictly contained in \mathcal{G} . \square

Theorem 5.2. *Let \mathcal{G} be a connected and reductive linear algebraic group defined over \mathbb{F}_q . Assume further that \mathcal{G} splits over \mathbb{F}_q , i.e., there exists a maximal torus T of \mathcal{G} that is defined over \mathbb{F}_q and splits over \mathbb{F}_q . Let \mathcal{H} be a closed subgroup of \mathcal{G} defined over $\overline{\mathbb{F}_q}((t))$ that contains a conjugate T^A of T for some $A \in \mathcal{G}(\mathbb{F}_q + t\overline{\mathbb{F}_q}[[t]])$ and such that every $g \in \mathcal{G}(\mathbb{F}_q)$ occurs as the constant part of an element inside $\mathcal{H}(\overline{\mathbb{F}_q}[[t]])$. Then $\mathcal{H} = \mathcal{G}$. In particular, $\langle T^A, \mathcal{G}(\mathbb{F}_q) \rangle$ is dense in \mathcal{G} for any $A \in \mathcal{G}(\mathbb{F}_q + t\overline{\mathbb{F}_q}[[t]])$.*

Proof. By Proposition 5.1 (with $K_1 = K_2 = \overline{\mathbb{F}_q}$), it is sufficient to show that for any $g \in \mathcal{G}(\overline{\mathbb{F}_q})$, there exists an element $h \in \mathcal{H}(\overline{\mathbb{F}_q}[[t]])$ with constant part g .

As the constant part A_0 of A is contained in $\mathcal{G}(\mathbb{F}_q)$, the maximal torus T^{A_0} is defined over \mathbb{F}_q and also splits over \mathbb{F}_q . Let $\Phi(\mathcal{G}, T^{A_0})$ denote the set of roots with respect to T^{A_0} and for $\alpha \in \Phi(\mathcal{G}, T^{A_0})$, let U_α be the root subgroup corresponding to α . Since T^{A_0} splits over \mathbb{F}_q , all root subgroups are defined over \mathbb{F}_q and we have isomorphisms

$$u_\alpha: \mathbb{G}_a \rightarrow U_\alpha$$

defined over \mathbb{F}_q for all $\alpha \in \Phi(\mathcal{G}, T^{A_0})$ (see [Bor91, V.18.7] for a proof). Now \mathcal{G} is generated by T^{A_0} together with all root subgroups (see [Spr09, 8.1.1]) and as all of these are defined over $\mathbb{F}_q \subseteq \overline{\mathbb{F}_q}$, we obtain

$$\begin{aligned} \mathcal{G}(\overline{\mathbb{F}_q}) &= \langle T^{A_0}(\overline{\mathbb{F}_q}), U_\alpha(\overline{\mathbb{F}_q}) \mid \alpha \in \Phi(\mathcal{G}, T^{A_0}) \rangle \\ &= \langle T(\overline{\mathbb{F}_q})^{A_0}, U_\alpha(\overline{\mathbb{F}_q}) \mid \alpha \in \Phi(\mathcal{G}, T^{A_0}) \rangle. \end{aligned}$$

Let now g be contained in $\mathcal{G}(\overline{\mathbb{F}_q})$. Then there exist an $r \in \mathbb{N}$, roots $\alpha_1, \dots, \alpha_r \in \Phi(\mathcal{G}, T^{A_0})$ (not necessarily pairwise distinct), $s_1, \dots, s_r \in \overline{\mathbb{F}_q}$ as well as $x_1, \dots, x_{r+1} \in T(\overline{\mathbb{F}_q})$ such that g can be written as

$$g = x_1^{A_0} u_{\alpha_1}(s_1) \cdots x_r^{A_0} u_{\alpha_r}(s_r) x_{r+1}^{A_0}.$$

Any root $\alpha \in \Phi(\mathcal{G}, T^{A_0})$ is a non-trivial character $\alpha: T^{A_0} \rightarrow \mathbb{G}_m$, hence it is surjective. As $u_\alpha(0) = 1$ holds for all $\alpha \in \Phi(\mathcal{G}, T^{A_0})$, we may assume that all s_1, \dots, s_r are contained in $\overline{\mathbb{F}_q}^\times$, so there exist elements $y_1^{A_0}, \dots, y_r^{A_0} \in T^{A_0}(\overline{\mathbb{F}_q})$ (that is, y_1, \dots, y_r are contained in $T(\overline{\mathbb{F}_q})$) such that

$$s_i = \alpha_i(y_i^{A_0})$$

for $1 \leq i \leq r$. The root subgroup isomorphisms u_α are subject to the relation

$$u_\alpha(\alpha(y)s) = u_\alpha(s)^y$$

for all elements y in the maximal torus and field elements s . Therefore, we have $u_{\alpha_i}(s_i) = u_{\alpha_i}(\alpha_i(y_i^{A_0}) \cdot 1) = u_{\alpha_i}(1)y_i^{A_0}$ for all $1 \leq i \leq r$ and thus

$$g = x_1^{A_0} (y_1^{A_0})^{-1} u_{\alpha_1}(1) y_1^{A_0} \cdots x_r^{A_0} (y_r^{A_0})^{-1} u_{\alpha_r}(1) y_r^{A_0} x_{r+1}^{A_0}.$$

As all isomorphisms u_{α_i} are defined over \mathbb{F}_q , we have $u_{\alpha_i}(1) \in \mathcal{G}(\mathbb{F}_q)$ for all $i \leq r$. By assumptions, there exist elements $h_1, \dots, h_r \in \mathcal{H}(\overline{\mathbb{F}_q}[[t]])$ such that the constant part of h_i equals $u_{\alpha_i}(1)$ for $1 \leq i \leq r$. Now consider

$$h := x_1^A (y_1^A)^{-1} h_1 y_1^A \cdots x_r^A (y_r^A)^{-1} h_r y_r^A x_{r+1}^A \in \mathcal{H}(\overline{\mathbb{F}_q}[[t]]).$$

Then the constant part of h equals g (recall that x_1 and y_1 are contained in $\mathcal{G}(\overline{\mathbb{F}_q})$). Hence $\mathcal{H} = \mathcal{G}$ holds.

As a special case, let $\mathcal{H} \subseteq \mathcal{G}$ be the Zariski closure of $\langle T^A, \mathcal{G}(\mathbb{F}_q) \rangle$. As A is contained in $\mathcal{G}(\overline{\mathbb{F}_q}((t)))$, we deduce that $T^A \cup \mathcal{G}(\mathbb{F}_q)$ is a closed subset of \mathcal{G} defined over $\overline{\mathbb{F}_q}((t))$. Therefore, \mathcal{H} is defined over $\overline{\mathbb{F}_q}((t))$ as well (see [Bor91, I.2.1(b)]). Hence \mathcal{H} conforms to the assumptions made in this Theorem, and $\mathcal{H} = \mathcal{G}$ follows. \square

The lower bound criterion Theorem 4.12 provides us with $\mathcal{G}(\overline{\mathbb{F}_q}[[t]])$ -conjugates of certain elements that are contained in the Galois group. Therefore, we have to descend from $\mathcal{G}(\overline{\mathbb{F}_q}[[t]])$ -conjugacy to $\mathcal{G}(\mathbb{F}_q + t \cdot \overline{\mathbb{F}_q}[[t]])$ -conjugacy in order to be able to apply Theorem 5.2.

Proposition 5.3. *Let $\mathcal{G} \leq \mathrm{GL}_n$ be a linear algebraic group defined over \mathbb{F}_q . Let g, h be contained in $\mathcal{G}(\mathbb{F}_q + t \cdot \overline{\mathbb{F}_q}[[t]])$. Assume that g is contained in a maximal torus T of \mathcal{G} defined over \mathbb{F}_q and that the centralizer of the constant part $g_0 \in T(\mathbb{F}_q)$ of g equals T . If g and h are conjugate over $\mathcal{G}(\overline{\mathbb{F}_q}[[t]])$ then they are already conjugate over $\mathcal{G}(\mathbb{F}_q + t \cdot \overline{\mathbb{F}_q}[[t]])$.*

Proof. Let $A \in \mathcal{G}(\overline{\mathbb{F}_q}[[t]])$ be such that $g^A = h$. As \mathcal{G} is defined over \mathbb{F}_q , the constant part A_0 of A is contained in $\mathcal{G}(\overline{\mathbb{F}_q})$. Similarly, the constant parts g_0 of g and h_0 of h are contained in $\mathcal{G}(\mathbb{F}_q)$. Then $g^A = h$ implies $g_0^{A_0} = h_0$ and applying ϕ_q on both sides yields $g_0^{\phi_q(A_0)} = g_0^{A_0}$. Applying the Lang isogeny ([Bor91, V.16.4]) to the centralizer T of g_0 , we obtain an element $y \in T(\overline{\mathbb{F}_q})$ satisfying $\phi_q(y)y^{-1} = \phi_q(A_0)A_0^{-1}$. Hence $y^{-1}A_0$ is contained in $\mathcal{G}(\mathbb{F}_q)$ and $h = g^A = g^{y^{-1}A}$ holds. The constant part of $y^{-1}A$ equals $y^{-1}A_0$ which is \mathbb{F}_q -rational. Hence h and g are conjugate over $\mathcal{G}(\mathbb{F}_q + t \cdot \overline{\mathbb{F}_q}[[t]])$. \square

6 The Main Result

In this section, we prove that every semisimple, simply-connected group defined over \mathbb{F}_q can be realized as a difference Galois group over $(\mathbb{F}_{q^i}(s, t), \phi_{q^i})$ for some $i \in \mathbb{N}$ using a result of Nori (Theorem 6.1) on finite Galois theory.

6.1 Finite Frobenius modules

A ϕ_q -difference module over $(\mathbb{F}_q(s), \phi_q)$ is called a *finite Frobenius module* over $(\mathbb{F}_q(s), \phi_q)$. Any finite Frobenius module has a unique Picard-Vessiot ring inside $\overline{\mathbb{F}_q}(s)^{\mathrm{sep}}$. The Picard-Vessiot ring E is then a finite Galois extension of $\mathbb{F}_q(s)$

which we call the Picard-Vessiot extension. The \mathbb{F}_q -rational points of the corresponding (finite) Galois group scheme $\mathcal{G} \leq \mathrm{GL}_n$ are isomorphic to $\mathrm{Gal}(E/F)$ via identifying $\gamma \in \mathrm{Gal}(E/F)$ with $Y^{-1}\gamma(Y) \in \mathcal{G}(\mathbb{F}_q)$, where $Y \in \mathrm{GL}_n(E)$ denotes a fixed fundamental solution matrix (see Proposition 2.13). We call $G = \mathcal{G}(\mathbb{F}_q)$ the Galois group of M . Every finite Galois extension can be obtained in this way using additive polynomials. Details can be found in [Mat04].

Theorem 6.1 (Nori). *Let \mathcal{G} be a semisimple, simply-connected linear algebraic group defined over \mathbb{F}_q . Then there exists a finite Frobenius module over $(\mathbb{F}_q(s), \phi_q)$ with representing matrix contained in $\mathcal{G}(\mathbb{F}_q(s))$, Picard-Vessiot extension $E/\mathbb{F}_q(s)$ linearly disjoint from $\overline{\mathbb{F}_q}$ over \mathbb{F}_q , and Galois group $\mathcal{G}(\mathbb{F}_q)$.*

Proof. Nori proved that there exists an absolutely irreducible unramified Galois covering of the affine line with Galois group $\mathcal{G}(\mathbb{F}_q)$ ([Nor94]). By Theorem 5.2. in [Mat04], there exists an effective, finite Frobenius module corresponding to the Galois covering provided by Theorem 6.1, i.e., the representing matrix can be chosen inside $\mathcal{G}(\mathbb{F}_q(s))$. The Picard-Vessiot extension E is linearly disjoint from $\overline{\mathbb{F}_q}$ over \mathbb{F}_q since the corresponding Galois covering is absolutely irreducible. \square

The following lower bound criterion for finite Frobenius modules due to Matzat can be found in [Mat04, Thm 4.5].

Theorem 6.2 (Matzat). *Let M be a finite Frobenius module over $(\mathbb{F}_q(s), \phi_q)$ with representing matrix $D \in \mathrm{GL}_n(\mathbb{F}_q(s))$ and Picard-Vessiot extension $E/\mathbb{F}_q(s)$. We fix a fundamental solution matrix $Y \in \mathrm{GL}_n(E)$. Let \mathfrak{p} be a place of degree d of $\mathbb{F}_q(s)$ with corresponding valuation ring $\mathfrak{o} \subseteq \mathbb{F}_q(s)$. If D is contained in $\mathrm{GL}_n(\mathfrak{o})$ then the following holds:*

- $E/\mathbb{F}_q(s)$ is unramified at \mathfrak{p} .
- For any extension $(\mathcal{O}, \mathcal{P})$ of $(\mathfrak{o}, \mathfrak{p})$ to E , Y is contained in $\mathrm{GL}_n(\mathcal{O})$.
- The Galois group $\mathrm{Gal}(E/\mathbb{F}_q(s)) \leq \mathrm{GL}_n(\mathbb{F}_q)$ of M contains the reduction of $Y^{-1}D\phi_q(D) \cdots \phi_{q^d-1}(D)Y$ modulo \mathcal{P} for any extension \mathcal{P} of \mathfrak{p} .

The following Proposition provides a converse to Theorem 6.2:

Proposition 6.3. *Let M be a finite Frobenius module over $(\mathbb{F}_q(s), \phi_q)$ with representing matrix $D \in \mathrm{GL}_n(\mathbb{F}_q(s))$, Picard-Vessiot extension $E/\mathbb{F}_q(s)$, and Galois group $G \leq \mathrm{GL}_n(\mathbb{F}_q)$. We fix a fundamental solution matrix $Y \in \mathrm{GL}_n(E)$. Let $g \in G$. Then there exist infinitely many places $(\mathfrak{o}, \mathfrak{p})$ of $\mathbb{F}_q(s)$ such that D is contained in $\mathrm{GL}_n(\mathfrak{o})$ and such that there is an extension $(\mathcal{O}, \mathcal{P})$ from $\mathbb{F}_q(s)$ to E where g equals the reduction of $Y^{-1}D\phi_q(D) \cdots \phi_{q^{\deg(\mathfrak{p})}-1}(D)Y \pmod{\mathcal{P}}$.*

Proof. We can write g as $g = Y^{-1}\gamma(Y)$ for an element $\gamma \in \mathrm{Gal}(E/\mathbb{F}_q(s))$. The proof of Theorem 6.2 (see [Mat04, Thm 4.5]) implies that we are looking for unramified finite places \mathfrak{p} of $\mathbb{F}_q(s)$ with extensions \mathcal{P} to E such that $D \in \mathrm{GL}_n(\mathfrak{o})$ and such that γ^{-1} is contained in the decomposition group of \mathcal{P}/\mathfrak{p} and acts as the Frobenius ϕ_{q^d} on \mathcal{O}/\mathcal{P} where d denotes the degree of \mathfrak{p} . The Chebotarev Density Theorem (see [FJ08, Thm 6.3.1]) implies that there exist infinitely many such places. \square

Proposition 6.4. *Let M be a finite Frobenius module over $(\mathbb{F}_q(s), \phi_q)$ with representing matrix $D \in \mathrm{GL}_n(\mathbb{F}_q(s))$, Picard-Vessiot extension $E/\mathbb{F}_q(s)$ and Galois group G . Assume that E and $\overline{\mathbb{F}_q}$ are linearly disjoint over \mathbb{F}_q . Then for any $i \geq 1$, the finite Frobenius module M_i over $(\mathbb{F}_{q^i}(s), \phi_{q^i})$ given by*

$$D_i := D\phi_q(D) \dots \phi_{q^{i-1}}(D)$$

has Picard-Vessiot extension $E\mathbb{F}_{q^i}$, and Galois group G .

Proof. Let $Y \in \mathrm{GL}_n(E)$ be a fundamental solution matrix for M . Hence $D\phi_q(Y) = Y$ which inductively implies $D_i\phi_{q^i}(Y) = Y$, so that Y is a fundamental solution matrix for M_i as well. As E is generated over $\mathbb{F}_q(s)$ by the entries of Y , we conclude that $E_i := E\mathbb{F}_{q^i}$ is generated over $\mathbb{F}_{q^i}(s)$ by the entries of Y . Hence E_i is a Picard-Vessiot extension of M_i and as E and \mathbb{F}_{q^i} are linearly disjoint over \mathbb{F}_q by assumption, we have $\mathrm{Gal}(E_i/\mathbb{F}_{q^i}(s)) = \mathrm{Gal}(E/\mathbb{F}_q(s)) = G$. \square

6.2 Lifting Nori's Theorem

Lemma 6.5. *Let \mathcal{G} be a connected, reductive linear algebraic group defined over \mathbb{F}_q of rank r . Assume that there exists a maximal torus T that splits over \mathbb{F}_q with \mathbb{F}_q -isomorphism $\gamma: \mathbb{G}_m^r \rightarrow T$. Then there exist irreducible polynomials $p_1, \dots, p_r \in \mathbb{F}_q[t]$ such that if we set $g = \gamma(p_1, \dots, p_r) \in T(\mathbb{F}_q(t))$ the following holds:*

- g is contained in $T(\mathbb{F}_q[t]_{(t)})$ and $g \equiv I \pmod{t}$.
- For any $g_0 \in T(\mathbb{F}_q)$, g_0g generates a dense subgroup of T . In particular, the centralizer of g_0g inside \mathcal{G} equals T .

Proof. Choose pairwise distinct irreducible polynomials $p_1, \dots, p_r \in \mathbb{F}_q[t]$ with constant terms 1 and set $g := \gamma(p_1, \dots, p_r)$. Then for any $g_0 \in T(\mathbb{F}_q)$ and every non-trivial character χ of T , we have $\chi(g_0g) \neq 1$ and g_0g thus generates a dense subgroup of T . \square

Theorem 6.6. *Let $\mathcal{G} \leq \mathrm{GL}_n$ be a semisimple, simply-connected linear algebraic group defined over \mathbb{F}_q . Then for a suitable $i \in \mathbb{N}$ there exists an n -dimensional difference module M over $(\mathbb{F}_{q^i}(s, t), \phi_{q^i})$ with a separable Picard-Vessiot ring $R/\mathbb{F}_{q^i}(s, t)$ and corresponding Galois group scheme isomorphic to \mathcal{G} (as linear algebraic group over $\mathbb{F}_{q^i}(t)$).*

Proof. By replacing q by a power q^i we may assume that there exists a maximal torus T of \mathcal{G} that splits over \mathbb{F}_q and such that $T(\mathbb{F}_q)$ contains a regular element g_0 . Then the dimension of the centralizer $\mathcal{C}_{\mathcal{G}}(g_0)$ equals r , the rank of \mathcal{G} . As \mathcal{G} is semisimple and simply-connected, all centralizers of semisimple elements are connected (see [Car85, Thm 3.5.6]), hence

$$\mathcal{C}_{\mathcal{G}}(g_0) = T. \tag{11}$$

Let $D'_0 \in \mathcal{G}(\mathbb{F}_q(s))$ be the representing matrix of the finite Frobenius module with Galois group $\mathcal{G}(\mathbb{F}_q)$ coming from Nori's theorem 6.1. Thanks to the Lang-isogeny, we can fix a fundamental solution matrix $Y_0 \in \mathcal{G}(\overline{\mathbb{F}_q(s)})^{\mathrm{sep}}$. We apply

Proposition 6.3 to $g = g_0$ and obtain a finite place \mathfrak{p}' of $\mathbb{F}_q(s)$ and an extension \mathcal{P}' to the Galois extension E corresponding to our finite Frobenius module. We define i to be the degree of \mathfrak{p}' . We then fix an extension \mathcal{P} of \mathcal{P}' from E to $E\mathbb{F}_{q^i}$ and set $\mathfrak{p} = \mathcal{P} \cap \mathbb{F}_{q^i}(s)$. We further define

$$D_0 = D'_0 \phi_q(D'_0) \dots \phi_{q^{i-1}}(D'_0) \in \mathcal{G}(\mathbb{F}_q(s)).$$

Then by Proposition 6.4, the finite Frobenius module M_0 over $(\mathbb{F}_{q^i}(s), \phi_{q^i})$ given by D_0 has Galois group $\mathcal{G}(\mathbb{F}_q)$ and Y_0 is still a fundamental solution matrix. By construction, the reduction of $Y_0^{-1} D_0 Y_0$ modulo \mathcal{P}' equals g_0 and so does the reduction modulo \mathcal{P} . Denote the reduction of D_0 modulo \mathfrak{p} by $\overline{D}_0 \in \mathcal{G}(\mathbb{F}_{q^i})$. Then \overline{D}_0 is conjugate to g_0 over $\mathcal{G}(\overline{\mathbb{F}_q})$ and in fact over $\mathcal{G}(\mathbb{F}_{q^i})$ by Equation (11) (compare Proposition 5.3). So we obtain an element $x \in \mathcal{G}(\mathbb{F}_{q^i})$ with

$$\overline{D}_0 = g_0^x. \quad (12)$$

Fix irreducible elements $p_1, \dots, p_r \in \mathbb{F}_q[t]$ as in Lemma 6.5 and set $g = \gamma(p_1, \dots, p_r) \in T(\mathbb{F}_q[t]_{(t)})$ (with $\gamma: \mathbb{G}_m^r \rightarrow T$ defined over \mathbb{F}_q). Then $g_0 g$ generates a dense subgroup of T and $g \equiv I \pmod{t}$. Fix a finite place $\mathfrak{q} \neq \mathfrak{p}$ of $\mathbb{F}_{q^i}(s)$ such that D_0 is contained in $\mathrm{GL}_n(\mathfrak{o}_{\mathfrak{q}})$, where $\mathfrak{o}_{\mathfrak{q}}$ denotes the corresponding valuation ring inside $\mathbb{F}_{q^i}(s)$. Let $f_{\mathfrak{q}} \in \mathbb{F}_{q^i}[s]$ be a generator of \mathfrak{q} . Recall that \mathfrak{p} is of degree 1 in $\mathbb{F}_{q^i}(s)$, hence there exists an $\alpha \in \mathbb{F}_{q^i}$ such that $\mathfrak{p} = (s - \alpha)$. Then $f_{\mathfrak{q}}(\alpha) \in \mathbb{F}_{q^i}^\times$, as we assumed $\mathfrak{q} \neq \mathfrak{p}$. Let $p_{jl} \in \mathbb{F}_q$ denote the coefficients of p_j , i.e.,

$$p_j = 1 + \sum_{l=1}^{n_j} p_{jl} t^l \in \mathbb{F}_q[t],$$

for all $1 \leq j \leq r$. We set

$$\tilde{p}_j = 1 + \sum_{l=1}^{n_j} p_{jl} \left(\frac{f_{\mathfrak{q}}}{f_{\mathfrak{q}}(\alpha)} \right)^l t^l \in \mathbb{F}_{q^i}[s][t],$$

for all $1 \leq j \leq r$. Note that $\tilde{p}_1, \dots, \tilde{p}_r$ are invertible inside $\mathbb{F}_{q^i}(s)[t]_{(t)}$, hence we can define

$$\tilde{g} := \gamma(\tilde{p}_1, \dots, \tilde{p}_r) \in T(\mathbb{F}_{q^i}(s)[t]_{(t)}).$$

We can now define the representing matrix $D \in \mathcal{G}(\mathbb{F}_{q^i}(s, t))$ of the desired difference module as

$$D = D_0 \tilde{g}^x \in \mathcal{G}(\mathbb{F}_{q^i}(s)[t]_{(t)})$$

with $D \equiv D_0 \pmod{t}$, as $\tilde{g} \equiv I \pmod{t}$. Let M be the corresponding difference module over $(\mathbb{F}_{q^i}(s, t), \phi_{q^i})$.

We first show that there exists a Picard-Vessiot extension for M . Let $|\cdot|$ be the absolute value on $k := \mathbb{F}_{q^i}(s)$ corresponding to \mathfrak{q} with $|f_{\mathfrak{q}}| = \frac{1}{2}$. We use the corresponding notation (such as K , $\mathcal{O}_{|\cdot|}$, \mathfrak{m} and L) set up in Section

3. By construction, the absolute value of the l -th coefficient of \tilde{p}_i is at most $(\frac{1}{2})^l$ and the same holds for \tilde{p}_i^{-1} (written as power series in t). Every entry of $\tilde{g} = \gamma(\tilde{p}_1, \dots, \tilde{p}_r)$ is given \mathbb{F}_q -polynomially in $\tilde{p}_1, \dots, \tilde{p}_r$ and their inverses, hence every entry of the l -th coefficient matrix \tilde{g}_l of \tilde{g} is bounded by $(\frac{1}{2})^l$, as well. We conclude

$$\|\tilde{g}_l\| \leq \left(\frac{1}{2}\right)^l$$

for every $l \in \mathbb{N}$. As x is contained in $\mathcal{G}(\mathbb{F}_{q^i})$, conjugating \tilde{g} with x is given \mathbb{F}_{q^i} -linearly in the entries of \tilde{g} and thus doesn't affect this convergence. Finally, we assumed $D_0 \in \mathrm{GL}_n(\mathfrak{o}_q)$, hence $\|D_0\| = 1$ and we conclude

$$\|D_l\| = \|D_0 \tilde{g}_l^x\| \leq \left(\frac{1}{2}\right)^l$$

for all $l \in \mathbb{N}$ (where $D_l \in \mathrm{M}_n(\mathbb{F}_{q^i}(s))$ denotes the l -th coefficient matrix of D). We can now apply Theorem 4.3 (with $\delta = \frac{1}{2}$) and obtain a fundamental solution matrix $Y \in \mathrm{GL}_n(\mathcal{O}_{|\cdot|}[[t]]) \cap \mathrm{M}_n(\mathcal{O}_{|\cdot|}\{t\})$. We apply Theorem 4.6 (note that $\mathcal{O}_{|\cdot|}/\mathfrak{m} \cong \overline{\mathbb{F}}_q$ embeds into K) and obtain another fundamental solution matrix Y' that is contained in $\mathcal{G}(L \cap \mathcal{O}_{|\cdot|}[[t]])$. Then the constant part Y'_0 of this new fundamental solution matrix is contained in $\mathcal{G}(K)$ and it is a fundamental solution matrix for D_0 . After multiplying Y' from the right with $Y_0'^{-1}Y_0 \in \mathcal{G}(\mathbb{F}_q)$, we may thus assume that the constant part of Y' equals our previously chosen Y_0 . From now on, we simply denote Y' by Y . Then $R := \mathbb{F}_{q^i}(s, t)[Y, Y^{-1}] \subseteq L$ is a Picard-Vessiot ring for M by Theorem 2.5. All entries of Y are actually contained in $\overline{\mathbb{F}}_q(s)^{\mathrm{sep}}((t))$ (and not just in $K((t))$ - compare the proof of Proposition 4.10). Now $\overline{\mathbb{F}}_q(s)^{\mathrm{sep}}((t))$ is separable over $\mathbb{F}_{q^i}(s)(t)$, hence $R/\mathbb{F}_{q^i}(s, t)$ is separable. We conclude that the Galois group scheme \mathcal{H} of M is a linear algebraic group (see Theorem 2.10) defined over $\mathbb{F}_{q^i}(t)$ and it is a closed subgroup of \mathcal{G} by Proposition 2.13.

We will now use the lower bound criterion 4.12 to show that $\mathcal{H} = \mathcal{G}$. By Theorem 5.2, it suffices to show that every element inside $\mathcal{G}(\mathbb{F}_q)$ occurs as a constant term inside $\mathcal{H}(\overline{\mathbb{F}}_q[[t]])$ and that \mathcal{H} contains a $\mathcal{G}(\mathbb{F}_q + t\overline{\mathbb{F}}_q[[t]])$ -conjugate of the \mathbb{F}_q -split torus T . The key point is to show that this is really a $\mathcal{G}(\mathbb{F}_q + t\overline{\mathbb{F}}_q[[t]])$ -conjugate and not just a $\mathcal{G}(\mathbb{F}_{q^i} + t\overline{\mathbb{F}}_q[[t]])$ -conjugate.

First of all, note that for any finite place \mathfrak{q}' of $\mathbb{F}_{q^i}(s)$ with valuation ring $\mathfrak{o}' \subseteq \mathbb{F}_{q^i}(s)$, the polynomials $\tilde{p}_1, \dots, \tilde{p}_r$ are contained in $(\mathfrak{o}'[t]_{(t)})^\times$. Hence $\tilde{g} = \gamma(\tilde{p}_1, \dots, \tilde{p}_r)$ and also \tilde{g}^x are contained in $\mathcal{G}(\mathfrak{o}'[[t]])$. We conclude that D is contained in $\mathcal{G}(\mathfrak{o}'[[t]])$ if and only if D_0 is contained in $\mathcal{G}(\mathfrak{o}')$.

Consider $\mathfrak{q}' = \mathfrak{p}$ with corresponding valuation ring \mathfrak{o} . Then D_0 is contained in $\mathcal{G}(\mathfrak{o})$ by the choice of \mathfrak{p} . Let \mathcal{O} be the (non-discrete) valuation ring inside $\overline{\mathbb{F}}_q(s)^{\mathrm{sep}}$ corresponding to a fixed extension $\tilde{\mathcal{P}}$ of \mathfrak{p} and let $\kappa: \mathcal{O}[[t]] \rightarrow \overline{\mathbb{F}}_q[[t]]$ denote the coefficient-wise reduction modulo $\tilde{\mathcal{P}}$. By Theorem 4.12 (with $k = \mathbb{F}_{q^i}(s)$),

$\mathcal{H}(\mathbb{F}_{q^i}[[t]])$ contains $h := \kappa(Y^{-1}DY)$ (since $d = 1$, as $\mathfrak{o}/\mathfrak{p} \cong \mathbb{F}_{q^i}$). We use $\kappa(s) = \alpha$, hence $\kappa(\tilde{p}_j) = p_j$ for all j to compute

$$\begin{aligned}\kappa(D) &= \kappa(D_0)\kappa(\tilde{g})^x \\ &= \overline{D_0}\gamma(\kappa(\tilde{p}_1), \dots, \kappa(\tilde{p}_r))^x \\ &= g_0^x \gamma(p_1, \dots, p_r)^x \\ &= (g_0 g)^x,\end{aligned}$$

where we also used Equation (12). Therefore, h is conjugate to $g_0 g$ via $x \cdot \kappa(Y)^{-1} \in \mathcal{G}(\overline{\mathbb{F}_q}[[t]])$. On the other hand, the constant term of h equals the reduction of $Y_0^{-1}D_0Y_0$ at \mathcal{P} , which equals g_0 by construction. Hence h is contained in $\mathcal{G}(\mathbb{F}_q + t\mathbb{F}_{q^i}[[t]])$ and is thus conjugate to $g_0 g \in \mathcal{G}(\mathbb{F}_q[[t]])$ not only over $\mathcal{G}(\overline{\mathbb{F}_q}[[t]])$ but also over $\mathcal{G}(\mathbb{F}_q + t\overline{\mathbb{F}_q}[[t]])$, by Proposition 5.3. Let $A \in \mathcal{G}(\mathbb{F}_q + t\overline{\mathbb{F}_q}[[t]])$ be such that $(g_0 g)^A = h$. Recall that $g_0 g$ generates a dense subgroup of T . Hence $h = (g_0 g)^A$ generates a dense subgroup of T^A , and \mathcal{H} thus contains T^A .

For the finite part, let $\xi \in \mathcal{G}(\mathbb{F}_q)$ be arbitrary and fix one of the finite places \mathfrak{p}_ξ of $\mathbb{F}_{q^i}(s)$ with extension \mathcal{P}_ξ provided by Proposition 6.3 applied to the finite Frobenius module M_0 over $(\mathbb{F}_{q^i}(s), \phi_{q^i})$. Let \mathfrak{o}_ξ denote the corresponding valuation ring inside $\mathbb{F}_{q^i}(s)$ and d_ξ the degree of \mathfrak{p}_ξ . Then $D_0 \in \mathcal{G}(\mathfrak{o}_\xi)$ and thus $D \in \mathcal{G}(\mathfrak{o}_\xi[[t]])$. Let further $\tilde{\mathcal{P}}_\xi$ be an extension of \mathcal{P}_ξ to $\overline{\mathbb{F}_q}(s)^{\text{sep}}$. Then by Theorem 4.12, $\mathcal{H}(\mathbb{F}_{q^i}[[t]])$ contains

$$\kappa_\xi(Y^{-1}D\phi_q(D) \dots \phi_{q^{d_\xi-1}}(D)Y),$$

where κ_ξ denotes the coefficient-wise reduction modulo $\tilde{\mathcal{P}}_\xi$. Looking at constant parts, we deduce that the reduction of

$$Y_0^{-1}D_0\phi_q(D_0) \dots \phi_{q^{d_\xi-1}}(D_0)Y_0 \mod \mathcal{P}_\xi$$

occurs as a constant term in $\mathcal{H}(\mathbb{F}_{q^i}[[t]])$. By construction, this reduction equals ξ . Hence every element in $\mathcal{G}(\mathbb{F}_q)$ occurs as a constant term inside $\mathcal{H}(\mathbb{F}_{q^i}[[t]])$ which concludes the proof. \square

6.3 Example

Let now $\mathcal{G} = \text{SL}_n$, assume $q > n(n+1)/2$, and let T be the $(\mathbb{F}_q$ -split) diagonal torus inside SL_n . If $\zeta \in \mathbb{F}_q$ is a $(q-1)$ -th primitive root of unity, then $T(\mathbb{F}_q)$ contains the regular element

$$g_0 := \text{diag}(\zeta, \zeta^2, \dots, \zeta^{n-1}, \zeta^{-\frac{n(n-1)}{2}}).$$

It was shown in [AM11] that there exists $f_i \in \mathbb{F}_q[s]$ of the form $f_i = s\alpha_i + (1-s)\beta_i$ for some $\alpha_i, \beta_i \in \mathbb{F}_q$ such that the finite Frobenius module over $(\mathbb{F}_q(s), \phi_q)$ given

by

$$D_0 = \begin{pmatrix} f_1 & \cdots & f_{n-1} & (-1)^{n-1} \\ 1 & & & \\ & \ddots & & \\ & & 1 & 0 \end{pmatrix}$$

has Galois group $\mathrm{SL}_n(\mathbb{F}_q)$. Let $\gamma_1, \dots, \gamma_{n-1}$ be the coefficients of the characteristic polynomial of g_0 . Fix an element $\alpha \in \mathbb{F}_q \setminus \{0, 1\}$. Then it is easy to see that if we alter f_i to

$$f_i = s\alpha_i + (1-s)\beta_i + \frac{s(s-1)}{\alpha(\alpha-1)}(\gamma_i - \alpha\alpha_i - (1-\alpha)\beta_i),$$

the corresponding Frobenius module M_0 over $(\mathbb{F}_q(s), \phi_q)$ has the same Galois group. For this new Frobenius module, there exists a place \mathfrak{p} of degree 1 of $\mathbb{F}_q(s)$, namely $\mathfrak{p} = (s - \alpha)$, such that the specialization of D_0 at \mathfrak{p} is conjugate to g_0 over $\mathcal{G}(\mathbb{F}_q)$. Hence the number i in Theorem 6.6 can be chosen as $i = 1$. The elements p_j in Lemma 6.5 can be chosen as $p_j = (1 + \zeta^j t)$ for $1 \leq j \leq n-1$. Following the proof of Theorem 6.6, we obtain that the difference module M over $(\mathbb{F}_q(s, t), \phi_q)$ given by

$$D = D_0 \cdot \mathrm{diag}(\tilde{p}_1, \dots, \tilde{p}_{n-1}, (\tilde{p}_1 \cdots \tilde{p}_{n-1})^{-1})^x$$

has Galois group SL_n where the elements $\tilde{p}_j \in \mathbb{F}_q[s, t]$ and $x \in \mathcal{G}(\mathbb{F}_q)$ can also be chosen explicitly: We fix the finite place $\mathfrak{q} = (s)$, hence $f_{\mathfrak{q}} = s$ and we can define \tilde{p}_j as

$$\tilde{p}_j := 1 + \zeta^j \frac{s}{\alpha} t$$

for $1 \leq j \leq n-1$. Finally, $x \in \mathrm{SL}_n(\mathbb{F}_q)$ is a matrix such that the reduction of $\overline{D_0}$ of D_0 at $\mathfrak{p} = (s - \alpha)$ equals g_0^x . We have

$$\overline{D_0} = \begin{pmatrix} \gamma_1 & \cdots & \gamma_{n-1} & (-1)^{n-1} \\ 1 & & & \\ & \ddots & & \\ & & 1 & 0 \end{pmatrix}$$

and it is easy to see that x can be chosen as

$$x = \begin{pmatrix} \det(A)^{-1} & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix} \cdot A$$

with A the Vandermonde-matrix corresponding to $(\zeta^{-1}, \zeta^{-2}, \dots, \zeta^{-n+1}, \zeta^{\frac{n(n-1)}{2}})$.

7 Pre- t -Motives

In this section, we lift our result from $k(t)$ to $\bar{k}(t)$ to get pre- t -motives with semisimple simply-connected Galois groups. Pre- t -motives are defined in Definition 7.2. For more information on the theory of t -motives, we refer the reader to [Pap08] and [Tae09] as well as to the survey articles [BP11] and [Cha10].

We first specify our notation as follows.

- k : $k = \mathbb{F}_q(\theta)$, a rational function field.
- $|\cdot|_\infty$: the ∞ -adic valuation on k with $|\theta|_\infty = q$.
- K, L : are as defined in Section 3 (with respect to $|\cdot|_\infty$).
- σ : on \bar{k} and K , σ is the inverse of the Frobenius and σ extends to $\bar{k}(t)$, $K\{t\}$ and L by acting coefficient-wise, i.e., $\sigma(t) = t$. Note that $L^\sigma = k^\sigma = \mathbb{F}_q(t)$ holds.

Definition 7.1. A pre- t -motive is a left $\bar{k}(t)[\sigma, \sigma^{-1}]$ -module that is finite dimensional over $\bar{k}(t)$. In other words, a pre- t -motive is a difference module (P, σ) over $(\bar{k}(t), \sigma)$ as defined in Definition 2.3. The notion “pre- t -motive” depends on q , since $\sigma = \phi_q^{-1}$. When considering pre- t -motives with respect to different q ’s at the same time, we will clarify this by calling a pre- t -motive corresponding to $\sigma = \phi_q^{-1}$ a pre- q - t -motive. If q has been fixed, a pre- q^i - t -motive is sometimes called a pre- t -motive of level i .

Definition 7.2. A pre- t -motive (P, σ) is called rigid analytically trivial, if $P \otimes_{\bar{k}(t)} L$ has a σ -invariant L -basis. In other words, P is rigid analytically trivial if and only if there exists a Picard-Vessiot ring of P contained in L .

The category of rigid analytically trivial pre- t -motives is a neutral Tannakian category over $\mathbb{F}_q(t)$ with fiber functor mapping a pre- t -motive (P, σ) to the vector space of solutions inside $P \otimes_F L$, i.e. the elements $\alpha \in P \otimes_F L$ with $\sigma \otimes \sigma(\alpha) = \alpha$ ([Pap08, 3.3.15]).

Theorem 7.3. Let $\mathcal{G} \leq \mathrm{GL}_n$ be a semisimple and simply-connected linear algebraic group defined over \mathbb{F}_q . Then there exists an $i \in \mathbb{N}$ and a pre- q^i - t -motive that is rigid analytically trivial and has Galois group isomorphic to \mathcal{G} as linear algebraic group over $\mathbb{F}_{q^i}(t)$.

Proof. We proved in Theorem 6.6 that there exists an $i \in \mathbb{N}$ and a difference module M over $(\mathbb{F}_{q^i}(s, t), \phi_{q^i})$ with Galois group \mathcal{G} . Recall that we constructed the Picard-Vessiot ring inside $L_{\mathfrak{q}}$, where \mathfrak{q} denotes a finite place inside $\mathbb{F}_q(s)$ and $L_{\mathfrak{q}}$ denotes the fraction field of $K_{\mathfrak{q}}\{t\}$ with $K_{\mathfrak{q}}$ the completion of an algebraic closure of the completion of k with respect to an absolute value coming from \mathfrak{q} . We may assume without loss of generality that \mathfrak{q} has degree 1 (by choosing a larger i in the proof of 6.6), hence \mathfrak{q} is of the form $(s - \alpha)$. We can now rename $\theta = \frac{1}{s - \alpha}$, i.e. we replace every occurrence of s in the representing matrix $D \in \mathrm{GL}_n(\mathbb{F}_{q^i}(s)(t))$ of M with $(\theta^{-1} + \alpha)$ and obtain a matrix $\Phi \in \mathrm{GL}_n(\mathbb{F}_{q^i}(\theta)(t))$. Hence we have found a difference module M over $(\mathbb{F}_{q^i}(\theta)(t), \phi_{q^i})$ with Galois group \mathcal{G} , fundamental solution matrix $Y \in \mathrm{GL}_n(L)$ and Picard-Vessiot ring

$R := k(t)[Y, Y^{-1}] \subseteq L$. Hence R and $\bar{k}(t)$ are both contained in L and the Galois group is connected, so we can apply Theorem 2.16 to conclude that $M \otimes_k \bar{k}$ has Picard-Vessiot ring $R \otimes_k \bar{k} = \bar{k}(t)[Y, Y^{-1}] \subseteq L$ over $\bar{k}(t)$ and also Galois group \mathcal{G} .

Let P be the pre- q^i - t -motive given by $\Phi \in \mathrm{GL}_n(\bar{k}(t))$ and set $\Psi = \phi_q(Y) \in \mathrm{GL}_n(L)$. As Y is a fundamental solution matrix for M , we have

$$\Phi \phi_q(Y) = Y$$

which translates to

$$\Phi \Psi = \sigma(\Psi).$$

Hence Ψ is a rigid analytic trivialization of P and

$$R \otimes_k \bar{k} = \bar{k}(t)[Y, Y^{-1}] = \bar{k}(t)[\Psi, \Psi^{-1}]$$

is also a Picard-Vessiot ring for P . Hence the Galois group schemes of P and $M \otimes_k \bar{k}$ coincide (they both equal $\underline{\mathrm{Aut}}(R \otimes_k \bar{k}/\bar{k}(t))$). \square

References

- [AM05] Katsutoshi Amano and Akira Masuoka. Picard-Vessiot extensions of Artinian simple module algebras. *J. Algebra*, 285(2):743–767, 2005.
- [AM11] Maximilian Albert and Annette Maier. Additive Polynomials for Finite Groups of Lie Type. *Israel J. Math.* 186(1), 125-195., 2011.
- [Bor91] Armand Borel. *Linear algebraic groups*, volume 126 of *Graduate Texts in Mathematics*. Springer, New York, second edition, 1991.
- [BP11] W. Dale Brownawell and Matthew A. Papanikolas. A rapid introduction to drinfeld modules t -modules and t -motives. *Preprint; available online*, 2011.
- [Car85] Roger W. Carter. *Finite groups of Lie type*. Pure and Applied Mathematics (New York). John Wiley & Sons Inc., New York, 1985. Conjugacy classes and complex characters, A Wiley-Interscience Publication.
- [Cha10] Chieh-Yu Chang. Frobenius difference equations and difference galois groups. *Preprint; available online*, 2010.
- [EP05] Antonio J. Engler and Alexander Prestel. *Valued fields*. Springer, Berlin, 2005.
- [FJ08] Michael D. Fried and Moshe Jarden. *Field arithmetic*. Springer, Berlin, third edition, 2008.
- [Kuh10] F.-V. Kuhlmann. Maps on ultrametric spaces, Hensel’s Lemma, and differential equations over valued fields. *To appear in: Comm. in Alg; available at arXiv:1003.5677v1*, 2010.

- [Lan02] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer, New York, third edition, 2002.
- [Mai11] Annette Maier. *Difference Equations with Semisimple Galois Groups in Positive Characteristic*. PhD Thesis, RWTH Aachen University (available at <http://darwin.bth.rwth-aachen.de/opus3/volltexte/2012/3909/>), 2011.
- [Mat01] B. Heinrich Matzat. *Differential Galois Theory in Positive Characteristic*. Notes from a class given by B.H. Matzat. IWR-Preprint No. 2001-35, available on <http://www.iwr.uni-heidelberg.de/organization/sfb359/Preprints2001.html>, 2001.
- [Mat04] B. Heinrich Matzat. Frobenius modules and Galois groups. In *Galois theory and modular forms*, volume 11, pages 233–267. Kluwer Acad. Publ., Boston, 2004.
- [Mat09] B. Heinrich Matzat. Frobenius modules and Galois representations. *Ann. Inst. Fourier (Grenoble)*, 59(7):2805–2818, 2009.
- [MS96] C. Mitschi and M. F. Singer. Connected linear groups as differential Galois groups. *J. Algebra*, 184(1):333–361, 1996.
- [Nor94] Madhav V. Nori. Unramified coverings of the affine line in positive characteristic. In *Algebraic geometry and its applications (West Lafayette, IN, 1990)*, pages 209–212. Springer, New York, 1994.
- [Pap08] Matthew A. Papanikolas. Tannakian duality for Anderson-Drinfeld motives and algebraic independence of Carlitz logarithms. *Invent. Math.*, 171(1):123–174, 2008.
- [Spr09] T. A. Springer. *Linear algebraic groups*. Birkhäuser Boston Inc., second edition, 2009.
- [Tae09] Lenny Taelman. Artin t -motifs. *J. Number Theory*, 129(1):142–157, 2009.
- [vdPS97] Marius van der Put and Michael F. Singer. *Galois theory of difference equations*, volume 1666 of *Lecture Notes in Mathematics*. Springer, Berlin, 1997.
- [vdPS03] Marius van der Put and Michael F. Singer. *Galois theory of linear differential equations*. Springer, Berlin, 2003.
- [Wib10] Michael Wibmer. *Geometric Difference Galois Theory*. PhD Thesis, Heidelberg, 2010.

*Lehrstuhl für Mathematik (Algebra), RWTH Aachen University,
52062 Aachen, Germany. email: annette.maier@matha.rwth-aachen.de*